Splunk® Enterprise
REST API Reference Manual 9.4.2

Generated: 4/28/2025 2:11 pm

Table of Contents

Introduction.....1

Using the REST API reference.....1

Endpoints reference list.....4

Access endpoints.....24

Access endpoint descriptions.....24

Application endpoints.....205

Application endpoint descriptions.....205

Cluster endpoints.....232

Cluster endpoint descriptions.....232

Configuration endpoints.....379

Configuration endpoint descriptions.....379

Deployment endpoints.....396

Deployment endpoint descriptions.....396

Federated Search endpoints.....455

Federated search endpoint descriptions.....455

Input endpoints.....519

Input endpoint descriptions.....519

Introspection endpoints.....686

Introspection endpoint descriptions.....686

Knowledge endpoints.....817

Knowledge endpoint descriptions.....817

KV store endpoints.....963

KV store endpoint descriptions.....963

License endpoints.....998

License endpoint descriptions.....998

Metrics Catalog endpoints.....1034

Metrics Catalog endpoint descriptions.....1034

Output endpoints.....1052

Output endpoint descriptions.....1052

Search endpoints.....1083

Search endpoint descriptions.....1083

Table of Contents

System endpoints....1294

System endpoint descriptions....1294

Workload management endpoints....1317

Workload management endpoint descriptions....1317

Introduction

Using the REST API reference

Use the REST API Reference to learn about available endpoints and operations for accessing, creating, updating, or deleting resources. See the REST API User Manual to learn about the Splunk REST API basic concepts.

Splunk Cloud Platform REST API usage

There are some REST API access and usage differences between Splunk Cloud Platform and Splunk Enterprise. If you are using Splunk Cloud Platform, review details in Access requirements and limitations for the Splunk Cloud Platform REST API.

Splunk REST API admin endpoints

Splunk does not support or document REST API endpoints that contain `/admin/` in their URIs. Use the corresponding publicly documented endpoint instead.

Resource groups

Resources are grouped into the following categories.

Category	Description
Access control	Authorize and authenticate users.
Federated search	Manage federated providers and federated indexes.
Knowledge	Define indexed and searched data configurations.
KV store	Manage app key-value store.
Metrics Catalog	Enumerate metrics and dimensions associated with metrics.
Search	Manage searches and search-generated alerts and view objects.

Splunk Cloud Platform supports a subset of the REST API endpoints available in Splunk Enterprise. For a full list of endpoints supported in Splunk Enterprise, see Resource groups in the *Splunk Enterprise REST API Reference Manual*.

See the Endpoints reference list for an alphabetical list of endpoints.

Available operations

Depending on the endpoint, GET, POST, and/or DELETE operations are available for accessing, creating, updating, or deleting resources. Some operations have specific capability requirements, as noted.

Using endpoint reference entries

Reference information for each endpoint in the REST API includes the following items.

- URL
- Usage details
- Expandable elements showing available operations (GET, POST, and/or DELETE) for the endpoint.

Expand a GET, POST, or DELETE element to show the following usage information about the operation.

- Request parameter information and requirements.
- Returned values included in the response.
- Example request and response.

Request and response details

Pagination and filtering parameters

In addition to the parameters specific to each endpoint and operation, the following request parameters are valid for some GET methods.

Name	Datatype	Default	Description
count	Number	`30`	Maximum number of entries to return. Set value to 0 to get all available entries.
f	String		Filters the response to include only the named values. Specify multiple times to return multiple values. Examples: `f=qualifiedSearch` returns only the value for `qualifiedSearch`. `f=s*` returns all the values that have names beginning with `s`. `f=qualifiedSearch&f=is_visible` returns the values for `qualifiedSearch` as well as `is_visible`.
offset	Number	`0`	Index of first item to return.
search	String		Response filter, where the response field values are matched against this search expression. Example: `search=foo` matches on any field with the string `foo` in the name. `search=field_name%3Dfield_value` restricts the match to a single field. (Requires URI-encoding.)
sort_dir	Enum	`asc`	Response sort order: `asc` = ascending `desc` = descending
sort_key	String	`name`	Field name to use for sorting.
sort_mode	Enum	`auto`	Collated ordering: `auto` = If all field values are numeric, collate numerically. Otherwise, collate alphabetically. `alpha` = Collate alphabetically, not case-sensitive. `alpha_case` = Collate alphabetically, case-sensitive. `num` = Collate numerically.
summarize	Bool	`false`	Response type:

Name	Datatype	Default	Description
			`true` = Summarized response, omitting some index details, providing a faster response. `false` = full response.

Returned values

The response to GET and other requests typically includes key-value pairs representing details about the resource that you are accessing. Returned values specific to the resource and/or operation are listed along with their descriptions.

HTTP status codes

Responses can include HTTP status codes. Standard HTTP status codes are not included in endpoint documentation, but status codes with specific meaning for an endpoint and/or operation are noted.

Error messages

Requests with an error, such as a missing required parameter, can prompt an error response like the following example.

```
<response>
  <messages>
    <msg type="ERROR">
      In handler 'datamodelgenerate': The following required arguments are missing: sid.
    </msg>
  </messages>
</response>
```

EAI response data

EAI response data, the `<eai:acl>` and `<eai:attributes>` elements, typically apply to all endpoints and are configuration-dependent, so redundant explanation is omitted. These elements are also elided from the response examples to make the documentation easier to read.

Access Control List (ACL) `[eai:acl]`

The REST implementation enforces ownership and permissions for a resource based on application context namespace. The ACL includes the following parameters.

Parameter	Description
app	The app context for the resource. Allowed values are: • The name of an app • `system`
can_list	For internal use only for the Splunk Web manager UI.
*can_share_**	Indicates whether or not the current user can change the sharing state. The sharing state can be one of: • `can_share_app` = App-level sharing • `can_share_global` = Global sharing • `can_share_user` = User-level sharing
can_write	Indicates whether or not the current user can edit this item.
owner	The user that owns the resource.

Parameter	Description
	A value of `nobody` indicates that all users have access to the resource, but that write access to the resource might be restricted.
modifiable	Indicates whether or not you can change the Access Control List (ACL). Set to false for items not controlled by ACLs, such as items under `/server/logger`.
perms.read	Properties that indicate read permissions of the resource.
perms.write	Properties that indicate write permissions of the resource.
removable	Indicates if an admin or user with sufficient permissions can remove the entity.
sharing	Indicates how the resource is shared. Allowed values are: • `app` = Shared through an app. • `global` = Shared to all apps. • `user` = Private to a user.

Note: You can append `/_acl` to an endpoint to access its ACL properties. For more information, see Access Control List in the *REST API User Manual*.

EAI attributes `[eai:attributes]`

The `eai:attributes` element shows the mandatory and optional fields.

Attribute	Description
optionalFields	Field is optional.
requiredFields	Field is required.
wildcardFields	Field can use wildcard.

References

See the following resources for more information on working with the Splunk REST API.

- *REST API User Manual*
- *REST API Tutorials*

Endpoints reference list

Navigate to specific endpoints and review available REST operations. Endpoints are listed alphabetically.

The PUT operation is not available for REST API endpoints. Depending on the endpoint, you can use a POST operation to create and/or update resources. Check specific endpoints for details.

Namespace access

Some resources in the REST API are associated with specific namespaced user and app contexts.

To access namespaces associated with all users, all apps, or resources shared by all users for an endpoint (similar to 'file globbing' or 'recursion' of input directories), make a GET request using `servicesNS` with wildcard `-` characters for the app and user. For example, use `/servicesNS/-/-/saved/searches`.

For more details, see Namespace in the *REST API User Manual*.

Endpoints

Jump to: A - C - D - I - L - M - P - R - S

URI	Summary	GET	PUT	POST	DEL
`admin/`					
admin/LDAP-groups	Access Manage LDAP authentication.				
admin/metrics-reload/_metrics	Access Reload the metrics processor after updating a metrics-related configuration.				
admin/ProxySSO-auth	Access Manage ProxySSO mappings and configurations.				
admin/replicate-SAML-certs	Access Manage SAML authentication.				
admin/Rsa-MFA	Access Configure RSA Multifactor Authentication.				
admin/Rsa-MFA-config-verify/<rsa-stanza-name>	Access Verify RSA multifactor authentication.				
admin/SAML-groups	Access Convert external groups in an IdP response to internal Splunk platform roles.				
admin/SAML-idp-metadata	Access Access IdP SAML metadata attributes.				
admin/SAML-sp-metadata	Access Access service provider SAML metadata attributes.				
admin/SAML-user-role-map	Access Access or create SAML user and role information for saved searches if your IdP does not support Attribute Query Requests.				
admin/SAML-user-role-map/{name}	Access Access or create SAML user and role information for saved searches if your IdP does not support Attribute Query Requests.				
`alerts/`		**GET**	**PUT**	**POST**	**DELETE**
alerts/alert_actions					

URI	Summary	GET	PUT	POST	DEL
	Search Access a list of alert actions				
alerts/fired_alerts	Search Access all fired alerts				
alerts/fired_alerts/{name}	Search Access specific fired alert				
apps/		**GET**	**PUT**	**POST**	**DELETE**
apps/appinstall	Applications Install app from URL or local file				
apps/apptemplates	Applications Access app templates for creating new apps				
apps/apptemplates/{name}	Applications Access particular app template				
apps/local	Applications Manage local apps				
apps/local/{name}	Applications Manage specific local app				
apps/local/{name}/package	Applications Archive an app				
apps/local/{name}/setup	Applications Access setup information for an app				
apps/local/{name}/update	Applications Access update information for an app				
authentication/		**GET**	**PUT**	**POST**	**DELETE**
auth/login	Access control Provide user authentication				
authentication/current-context	Access control Access current user contexts				
authentication/current-context/{name}	Access control Access specific user context				
authentication/httpauth-tokens	Access control Manage session tokens				
authentication/httpauth-tokens/{name}	Access control Manage specific session token				
authentication/LDAP-auth	Access Create and manage LDAP strategies.				
authentication/providers/SAML	Access control Access and create SAML configurations.				
authentication/providers/SAML/{stanza_name}	Access control Access and update SAML configurations.				
authentication/users	Access control Manage user accounts				

URI	Summary	GET	PUT	POST	DEL
authentication/users/{name}	Access control Manage specific user account				
authorization/		**GET**	**PUT**	**POST**	**DELETE**
authorization/capabilities	Access control Access capability authorization				
authorization/grantable_capabilities	Access control Access capabilities that current user can grant.				
authorization/roles	Access control Access user roles				
authorization/roles/{name}	Access control Access specific user role				
authorization/tokens	Access control Access authentication tokens				
authorization/tokens/{user}	Access control Access authentication tokens for a specific user				
catalog/		**GET**	**PUT**	**POST**	**DELETE**
catalog/metricstore/metrics	Metrics List metric names.				
catalog/metricstore/dimensions	Metrics List dimension names.				
catalog/metricstore/dimensions/{dimension-name}/values	Metrics List values for given dimensions.				
catalog/metricstore/rollup	Metrics Retrieve lists of metric indexes and their rollup summaries. Create new rollup policies for a given metric index.				
catalog/metricstore/rollup/{index}	Metrics Manage rollup summaries and rollup policies associated with a specific source `{index}`.				
cluster/		**GET**	**PUT**	**POST**	**DELETE**
cluster/config	Clusters Access cluster configuration				
cluster/config/config	Clusters Manage cluster configuration				
cluster/manager/buckets	Clusters Access manager node bucket configurations				
cluster/manager/buckets/{name}	Clusters Access specific bucket configuration, manager node				
cluster/manager/control/control/rebalance_primaries	Clusters Access manager controls to rebalance primary				

URI	Summary	GET	PUT	POST	DEL
	buckets across peers				
cluster/manager/control/control/remove_peers	Clusters Remove disabled peer nodes.				
cluster/manager/control/control/roll-hot-buckets	Clusters Force a specified bucket in an indexer cluster to roll from hot to warm.				
cluster/manager/control/control/rolling_upgrade_finalize	Clusters Finalizes indexer cluster rolling upgrade.				
cluster/manager/control/control/rolling_upgrade_init	Clusters Initializes indexer cluster rolling upgrade.				
cluster/manager/generation	Clusters Access current generations information, manager node				
cluster/manager/generation/{name}	Clusters Access specific generation information, cluster manager				
cluster/manager/indexes	Clusters Access cluster index information				
cluster/manager/indexes/{name}	Clusters Access specific cluster index information				
cluster/manager/info	Clusters Access cluster manager node information				
cluster/manager/health	Clusters Performs health checks				
cluster/manager/peers	Clusters Access peer information, manager node				
cluster/manager/peers/{name}	Clusters Access specific manager node peer information				
cluster/manager/redundancy	Clusters Display the details of all cluster managers participating in cluster manager redundancy, and switch the HA state of the cluster managers.				
cluster/manager/sites	Clusters Access cluster site information				
cluster/manager/sites/{name}	Clusters Access specific cluster site information				
cluster/manager/status	Clusters Status of rolling restart				
cluster/searchhead/generation	Clusters Access searchhead peer information				
cluster/searchhead/generation/{name}	Clusters Access specific searchhead peer information				
cluster/searchhead/searchheadconfig	Clusters Access cluster configuration for searchhead				

URI	Summary	GET	PUT	POST	DEL
cluster/searchhead/searchheadconfig/{name}	Clusters Access specific cluster node				
cluster/peer/buckets	Clusters Access peer bucket configuration information				
cluster/peer/buckets/{name}	Clusters Access specific peer bucket configuration information				
cluster/peer/control/control/decommission	Clusters Decommission indexer cluster peer node				
cluster/peer/control/control/set_manual_detention	Clusters Configure indexer detention.				
cluster/peer/info	Clusters Access peer node information				
cluster/peer/info/{name}	Clusters Access information about specific peer				
`configs/`		**GET**	**PUT**	**POST**	**DELETE**
configs/conf-{file}	Configuration Raw access to `.conf` files				
configs/conf-{file}/{name}	Configuration Raw access to specific `.conf` file				
`data/`		**GET**	**PUT**	**POST**	**DELETE**
data/commands	Search Access search commands				
data/commands/{name}	Search Access specific search command				
data/index-volumes	Indexes Access logical drive information				
data/index-volumes/{name}	Indexes Access information for a logical drive				
data/indexes	Indexes Manage data indexes				
data/indexes/{name}	Indexes Manage specific data index				
data/indexes-extended	Indexes Access index bucket level information				
data/indexes-extended/{name}	Indexes Access specific index bucket level information				
data/ingest/rfsdestinations	Inputs Create/configure, get, or delete an S3 destination for ingest action.				
data/ingest/rulesets	Inputs Retrieve a list of rulesets.				
data/ingest/rulesets/{name}	Inputs Retrieve a particular ruleset.				

URI	Summary	GET	PUT	POST	DEL
data/ingest/rulesets/publish	Inputs Publish ruleset changes on the indexer cluster manager.				
data/inputs/ad	Inputs Access Active Directory monitoring input				
data/inputs/ad/{name}	Inputs Access Active Directory monitoring stanza				
data/inputs/all	Inputs Access all inputs, including Modular Inputs				
data/inputs/all/{name}	Inputs Access specific input				
data/inputs/http	Input Configure HTTP Event Collection.				
data/inputs/http/{name}	Input Configure HTTP Event Collection.				
data/inputs/monitor	Inputs Access monitor inputs				
data/inputs/monitor/{name}	Inputs Manage specific monitor input				
data/inputs/monitor/{name}/members	Inputs Access files for the specific monitor input				
data/inputs/oneshot	Inputs Access one-shot inputs				
data/inputs/oneshot/{name}	Inputs Access specific one-shot input information				
data/inputs/registry	Inputs Access Windows registry monitor input				
data/inputs/registry/{name}	Inputs Manage Windows registry monitor stanza				
data/inputs/script	Inputs Manage scripted inputs settings				
data/inputs/script/restart	Inputs Restart scripted input				
data/inputs/script/{name}	Inputs Manage specific scripted input				
data/inputs/tcp/cooked	Inputs Access forwarder TCP inputs				
data/inputs/tcp/cooked/{name}	Inputs Manage TCP inputs for specific host:port				
data/inputs/tcp/cooked/{name}/connections	Inputs Access connections for specific port				
data/inputs/tcp/raw	Inputs Manage raw forwarder TCP inputs				

URI	Summary	GET	PUT	POST	DEL
data/inputs/tcp/raw/{name}	Inputs Access raw TCP input information				
data/inputs/tcp/raw/{name}/connections	Inputs Manage raw TCP input information for specific host:port				
data/inputs/tcp/splunktcptoken	Inputs Manage receiver access using tokens.				
data/inputs/tcp/splunktcptoken/{name}	Inputs Manage existing receiver tokens.				
data/inputs/tcp/ssl	Inputs Access SSL configuration information				
data/inputs/tcp/ssl/{name}	Inputs Access SSL configuration for specific host				
data/inputs/token/http	Inputs Access http inputs				
data/inputs/token/http/{name}	Inputs Manage specific http input				
data/inputs/token/http/{name}/enable	Inputs Enable the {name} HTTP Event Collector token.				
data/inputs/token/http/{name}/disable	Inputs Disable the {name} HTTP Event Collector token.				
data/inputs/udp	Inputs Access UDP inputs				
data/inputs/udp/{name}	Inputs Manage specific UDP input				
data/inputs/udp/{name}/connections	Inputs Manage specific UDP input connection				
data/inputs/win-event-log-collections	Inputs Access all configured event log collections				
data/inputs/win-event-log-collections/{name}	Inputs Manage specific event log				
data/inputs/win-perfmon	Inputs Access Windows performance monitor information				
data/inputs/win-perfmon/{name}	Inputs Manage specific performance monitor configuration stanza				
data/inputs/win-wmi-collections	Inputs Access configured WMI collections				
data/inputs/win-wmi-collections/{name}	Inputs Manage specific WMI collection				
data/lookup-table-files	Knowledge Access lookup table files				

URI	Summary	GET	PUT	POST	DEL
data/lookup-table-files/{name}	Knowledge Manage specific lookup table file				
data/modular-inputs	Inputs Access defined modular inputs				
data/modular-inputs/{name}	Inputs Manage specific modular input				
data/outputs/tcp/default	Outputs Access global TCP output properties				
data/outputs/tcp/default/{name}	Outputs Manage specific TCP output property setting				
data/outputs/tcp/group	Outputs Access data forwarding group configurations				
data/outputs/tcp/group/{name}	Outputs Manage specific data forwarding group				
data/outputs/tcp/server	Outputs Access data forwarding configurations				
data/outputs/tcp/server/{name}	Outputs Manage specific forwarder configuration				
data/outputs/tcp/server/{name}/allconnections	Outputs Access current connections for specific forwarder				
data/outputs/tcp/syslog	Outputs Access forwarded server configured to provide data in standard syslog format				
data/outputs/tcp/syslog/{name}	Outputs Manage specific forwarder, which sends data in syslog format				
data/props/calcfields	Knowledge Access `props.conf` file calculated fields				
data/props/calcfields/{name}	Knowledge Manage specific `props.conf` file calculated field				
data/props/extractions	Knowledge Access `props.conf` file search-time field extractions				
data/props/extractions/{name}	Knowledge Manage specific `props.conf` file field extraction				
data/props/fieldaliases	Knowledge Access `props.conf` file field aliases				
data/props/fieldaliases/{name}	Knowledge Manage specific `props.conf` file field alias				
data/props/lookups	Knowledge Access `props.conf` file automatic lookups				

URI	Summary	GET	PUT	POST	DEL
data/props/lookups/{name}	Knowledge Manage specific `props.conf` file automatic lookup				
data/props/sourcetype-rename	Knowledge Access renamed sourcetypes configured in `props.conf` file				
data/props/sourcetype-rename/{name}	Knowledge Manage specific `props.conf` file sourcetype name				
data/summaries	Introspection Get disk usage information about all summaries in an indexer.				
data/summaries/{summary_name}	Introspection Get disk usage information about a particular summary in an indexer.				
data/transforms/extractions	Knowledge Access field extraction definitions				
data/transforms/extractions/{name}	Knowledge Manage specific field extraction definition				
data/transforms/lookups	Knowledge Access `transforms.conf` file lookup definitions				
data/transforms/lookups/{name}	Knowledge Manage specific `transforms.conf` file lookup definition				
data/transforms/metric-schema	Knowledge Review and manage ingest-time log-to-metrics configurations.				
data/transforms/statsdextractions	Knowledge Configure metrics dimension extraction for StatsD.				
data/ui/global-banner	Knowledge Create global banners.				
data/ui/panels	Knowledge Create dashboard panel XML definitions.				
data/ui/views	Knowledge Create dashboard XML definitions.				
data/ui/views/{name}	Knowledge Access, update, or delete dashboard XML.				
`datamodel/`		**GET**	**PUT**	**POST**	**DELETE**
datamodel/model	Knowledge Access information about data models				
datamodel/model/{name}	Knowledge Access information about a data model				

URI	Summary	GET	PUT	POST	DEL
datamodel/pivot	Knowledge Access pivots based on named data models				
deployment/		**GET**	**PUT**	**POST**	**DELETE**
deployment/client	Deployment Access deployment client information				
deployment/client/config	Deployment Access deployment client configuration				
deployment/client/config/listIsDisabled	Deployment Access deployment client state information				
deployment/client/config/reload	Deployment Access deployment client reload information				
deployment/client/{name}/reload	Deployment Manage specific deployment client reload				
deployment/server/applications	Deployment Access deployment server application and class information				
deployment/server/applications/{name}	Deployment Manage specific server client application and class information				
deployment/server/clients	Deployment Access deployment server client information				
deployment/server/clients/countClients_by_machineType	Deployment Access deployment server client information by machine type				
deployment/server/clients/countRecentDownloads	Deployment Access client download information				
deployment/server/clients/{name}	Deployment Manage specific client				
deployment/server/config	Deployment Access deployment server configuration				
deployment/server/config/attributesUnsupportedInUI	Deployment Access deployment server attributes not available using Splunk Web				
deployment/server/config/listIsDisabled	Deployment Access deployment server state				
deployment/server/serverclasses	Deployment Access server class information				
deployment/server/serverclasses/{name}	Deployment Manage specific server class of deployment server				
deployment/server/serverclasses/rename	Deployment Manage server class name				
directory/		**GET**	**PUT**	**POST**	**DELETE**
directory	Knowledge Access user-configurable entities				

URI	Summary	GET	PUT	POST	DEL
directory/{name}	Knowledge Manage specific entity in directory service enumeration				
indexing/		**GET**	**PUT**	**POST**	**DELETE**
indexing/preview	Deployment Preview events from a file before indexing				
indexing/preview/{job_id}	Inputs Access `props.conf` file settings for specific data preview job				
kvstore/		**GET**	**PUT**	**POST**	**DELETE**
kvstore/backup/create	KV store Create a KV Store backup archive file.				
kvstore/backup/restore	KV store Extracts the KV Store backup archive file and restores the KV Store.				
kvstore/status	KV store Access KV store status information for standalone or search head clustering (SHC) deployments.				
licenser/		**GET**	**PUT**	**POST**	**DELETE**
licenser/groups	Licensing Access licenser groups configuration				
licenser/groups/{name}	Licensing Manage specific licenser group configuration				
licenser/licenses	Licensing Access licenses				
licenser/licenses/{name}	Licensing Manage specific license				
licenser/localpeer	Licensing Get information about relevant license state for the splunk instance.				
licenser/messages	Licensing Access licenser messages				
licenser/messages/{name}	Licensing Access specific licenser message				
licenser/pools	Licensing Access licenser pool information				
licenser/pools/{name}	Licensing Manage specific licenser pool				
licenser/peers	Licensing Access license manager peers				
licenser/peers/{name}	Licensing Access specific license manager peer				
licenser/stacks					

URI	Summary	GET	PUT	POST	DEL
	Licensing Access license stack configuration				
licenser/stacks/{name}	Licensing Access specific license stack configuration				
licenser/usage	Licensing Access current usage information.				
messages/		**GET**	**PUT**	**POST**	**DELETE**
messages	System Manage system messages				
messages/{name}	System Manage specific system message				
properties/		**GET**	**PUT**	**POST**	**DELETE**
properties	Configuration Access configuration files				
properties/{file_name}	Configuration Manage specific configuration file				
properties/{file_name}/{stanza_name}	Configuration Manage specific configuration file stanzas				
properties/{file_name}/{stanza_name}/{key_name}	Configuration Manage specific stanza in specific configuration file				
receivers/		**GET**	**PUT**	**POST**	**DELETE**
receivers/simple	Inputs Use HTTP to send events				
receivers/stream	Inputs Use socket to stream events				
receivers/token	Input Log events using HTTP Input with application authentication token.				
receivers/token/event	Input Post JSON formatted data to the data input endpoint.				
receivers/token/event/1.0	Input Post JSON formatted data to the data input endpoint.				
receivers/token/mint	Input Post MINT formatted data to the data input endpoint.				
receivers/token/mint/1.0	Input Post MINT formatted data to the data input endpoint.				
saved/		**GET**	**PUT**	**POST**	**DELETE**
saved/eventtypes	Knowledge Manage saved event types				

URI	Summary	GET	PUT	POST	DEL
saved/eventtypes/{name}	Knowledge Manage specific saved event type				
saved/searches	Search Manage saved searches configuration				
saved/searches/{name}	Search Manage specific saved search				
saved/searches/{name}/acknowledge	Search Manage saved search alerting				
saved/searches/{name}/dispatch	Search Dispatch saved search				
saved/searches/{name}/history	Search Access saved search job history				
saved/searches/{name}/reschedule	Search Manage saved search job scheduling				
saved/searches/{name}/scheduled_times	Search Access saved search scheduled times				
saved/searches/{name}/suppress	Search Access saved search alerting state				
scheduled/		**GET**	**PUT**	**POST**	**DELETE**
scheduled/views	Search Access scheduled views for PDF delivery				
scheduled/views/{name}	Search Manage specific scheduled view				
scheduled/views/{name}/dispatch	Search Dispatch search for specific scheduled view				
scheduled/views/{name}/history	Search Access specific scheduled view job history				
scheduled/views/{name}/reschedule	Search Manage scheduled view scheduling				
scheduled/views/{name}/scheduled_times	Search Access specific scheduled view times				
search/		**GET**	**PUT**	**POST**	**DELETE**
search/concurrency-settings	Search List search concurrency settings.				
search/concurrency-settings/scheduler	Search Edit settings for concurrent scheduled search limits.				
search/concurrency-settings/search	Search Edit settings for the maximum number of concurrent scheduled searches.				
search/distributed/bundle/replication/config	Deployment Provides information on knowledge bundle replication configuration				
search/distributed/bundle/replication/cycles					

URI	Summary	GET	PUT	POST	DEL
	Deployment Provides information and status for knowledge bundle replication cycles				
search/distributed/bundle-replication-files	Deployment Access distributed search bundle replication files				
search/distributed/bundle-replication-files/{name}	Deployment Access specific search bundle replication file				
search/distributed/config	Deployment Access distributed search options				
search/distributed/peers	Deployment Manage distributed server peers				
search/distributed/peers/{name}	Deployment Manage distributed server peers				
search/fields	Knowledge Access search field configuration				
search/fields/{field_name}	Knowledge Access specific search field configuration				
search/fields/{field_name}/tags	Knowledge Manage tags associated with specific search field				
search/jobs	Search Manage search jobs				
search/jobs/{search_id}	Search Manage specific search job				
search/jobs/{search_id}/control	Search Execute job control command for specific search				
search/jobs/{search_id}/events	Search Access events for specific search				
search/jobs/{search_id}/results	Search Access results of specific search				
search/jobs/{search_id}/results_preview	Search Access preview results for specific search				
search/jobs/{search_id}/search.log	Search Access `search.log` file for specific search				
search/jobs/{search_id}/summary	Search Access `getFieldsAndStats` output of so-far-read events				
search/jobs/{search_id}/timeline	Search Access event distribution over time				
search/jobs/export	Search Stream search results				
search/parser	Search Access search language parsing services				

URI	Summary	GET	PUT	POST	DEL
search/scheduler	Search Access search scheduler enablement status.				
search/scheduler/status	Search Disable or enable the search scheduler.				
search/tags/{tag_name}	Knowledge Manage specific search time tag				
search/timeparser	Search Parse time argument				
search/typeahead	Search Suggest search string auto-completion strings				
`server/`		**GET**	**PUT**	**POST**	**DELETE**
server/control	System Access server controls				
server/control/restart	System Restart Splunk Enterprise splunkd server daemon.				
server/control/restart_webui	System Restart Splunk Enterprise splunkweb Web interface process.				
server/httpsettings/proxysettings	System Create an HTTP proxy configuration stanza.				
server/httpsettings/proxysettings/proxyConfig	System Update HTTP proxy settings.				
server/info	Introspection Access Splunk instance information				
server/sysinfo	Introspection Access server information				
server/health/deployment	Introspection Access distributed deployment overall health status information.				
server/health/deployment/details	Introspection Access distributed deployment feature health status information.				
server/health/splunkd	Introspection Access `splunkd` health status information.				
server/health/splunkd/details	Introspection Access `splunkd` feature health status information.				
server/health-config	Introspection Access `splunkd` health report configuration information.				
server/health-config/{alert_action}	Introspection Configure alert actions for the `splunkd` health report.				
server/health-config/{feature_name}					

URI	Summary	GET	PUT	POST	DEL
	Introspection Edit feature and indicator settings for the `splunkd` health report.				
server/introspection	Introspection List introspection resources				
server/introspection/indexer	Introspection Get indexer status				
server/introspection/kvstore	Introspection List app kvstore status resources				
server/introspection/kvstore/collectionstats	Introspection Get storage statistics for a collection.				
server/introspection/kvstore/replicasetstats	Introspection Get the status of the replica set from the point of view of the current server.				
server/introspection/kvstore/serverstatus	Introspection Get an overview of the database process state.				
server/introspection/search/saved	Introspection Check most recent search scheduling details.				
server/logger	System Access logging categories				
server/logger/{name}	System Manage specific logging category				
server/pipelinesets	Input Access information on an indexer's ingestion pipeline sets.				
server/roles	System Access server configuration				
server/security/rotate-splunk-secret	System Rotate the `splunk.secret` key file on a standalone Splunk Enterprise installation				
server/settings	System Access server configuration				
server/status	Introspection Access system status information				
server/status/dispatch-artifacts	Introspection Access search job information				
server/status/fishbucket	Introspection Access information about the private BTree database				
server/status/installed-file-integrity	Introspection Check for system file irregularities.				
server/status/limits/search-concurrency	Introspection Access search concurrency metrics				
server/status/partitions-space	Introspection Access disk utilization information				

URI	Summary	GET	PUT	POST	DEL
server/status/resource-usage	Introspection Access current resource utilization information				
server/status/resource-usage/hostwide	Introspection Access host-level resource utilization information				
server/status/resource-usage/iostats	Introspection Access the most recent disk I/O statistics for each disk. This endpoint is currently available only for Linux.				
server/status/resource-usage/splunk-processes	Introspection Access operating system resource utilization information				
services/collector		**GET**	**PUT**	**POST**	**DELETE**
services/collector	Input Log events using HTTP Event Collector.				
services/collector/ack	Input Query event indexing status.				
services/collector/event	Input Post JSON formatted data to the data input endpoint.				
services/collector/health	Input Checks if HEC is healthy and able to accept new data from a load balancer.				
services/collector/mint	Input Post MINT formatted data to the data input endpoint.				
services/collector/raw	Input Send raw data directly to the indexer queue.				
shcluster/		**GET**	**PUT**	**POST**	**DELETE**
shcluster/captain/artifacts	Clusters Get artifact configuration information for a cluster captain node.				
shcluster/captain/artifacts/{name}	Clusters Get artifact configuration information for `{name}` node.				
shcluster/captain/control/control/upgrade-init	Clusters Initiate rolling upgrade of SHC.				
shcluster/captain/control/control/upgrade-finalize	Clusters Finish rolling upgrade of SHC.				
shcluster/captain/control/control/rotate-splunk-secret	System Rotate the `splunk.secret` key file on all nodes of a Splunk Enterprise search head cluster				
shcluster/captain/control/default/restart	Clusters Initiate rolling restart of SHC.				

URI	Summary	GET	PUT	POST	DEL
shcluster/captain/info	Clusters Access information about searchhead cluster captain node.				
shcluster/captain/jobs	Clusters List running and recently finished jobs for all cluster members.				
shcluster/captain/jobs/{name}	Clusters Get running and recently finished jobs for {name} cluster.				
shcluster/captain/members	Clusters List cluster members.				
shcluster/captain/members/{name}	Clusters Get information about the {name} searchhead cluster member.				
shcluster/config	Clusters List searchhead cluster node configuration.				
shcluster/config/config	Clusters Configure search head cluster members.				
shcluster/member/artifacts	Clusters Get searchhead cluster member artifact configuration.				
shcluster/member/artifacts/{name}	Clusters Get {name} member artifact configuration.				
shcluster/member/consensus	Clusters Get latest cluster configuration from the raft consensus protocol.				
shcluster/member/control/control/set_manual_detention	Clusters Adjust search head manual detention mode.				
shcluster/member/info	Clusters Get searchhead cluster member node information.				
shcluster/status	Clusters Determine SHC health status.				
replication/configuration/health	Clusters Get configuration replication health statistics for a SHC.				
storage/		**GET**	**PUT**	**POST**	**DELETE**
storage/passwords	Access control Manage authentication credentials				
storage/passwords/{name}	Access control Manage specific authentication credential				
storage/collections		**GET**	**PUT**	**POST**	**DELETE**
storage/collections/config	KV store Create or list connections.				
storage/collections/config/{collection}					

URI	Summary	GET	PUT	POST	DEL
	KV store Manage a specific collection.				
storage/collections/data/{collection}	KV store Manage items of a collection.				
storage/collections/data/{collection}/{id}	KV store Manage a specific item of a collection.				
storage/collections/data/{collection}/batch_save	KV store Perform multiple save operations.				
workloads/		**GET**	**PUT**	**POST**	**DELETE**
workloads/categories	Workloads List and edit workload categories.				
workloads/config/enable	Workloads Enable workload management.				
workloads/config/disable	Workloads Disable workload management.				
workloads/config/get-base-dirname	Workloads Get the name of the splunk parent cgroup.				
workloads/config/set-base-dirname	Workloads Set the name of the splunk parent cgroup.				
workloads/status	Workloads Get information on the current status of workload management.				
workloads/pools	Workloads Perform CRUD operations on workload pools.				
workloads/rules	Workloads Perform CRUD operations on workload rules.				

Access endpoints

Access endpoint descriptions

Access and manage user credentials.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform URL for REST API access

Splunk Cloud Platform has a different host and management port syntax than Splunk Enterprise. Use the following URL for Splunk Cloud Platform deployments. If necessary, submit a support case using the Splunk Support Portal to open port 8089 on your deployment.

```
https://<deployment-name>.splunkcloud.com:8089
```

Free trial Splunk Cloud Platform accounts cannot access the REST API.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the *REST API Tutorials* manual for more information.

admin/Duo-MFA

Configure Duo Multifactor authentication.

Authentication and Authorization
Requires the `change_authentication` capability.

Usage details
Disable any SSO configurations, such as SAML, before enabling Duo authentication for the first time. Duo only works with

local auth types.

GET

List Duo Multifactor configuration settings.

Request parameters
None

Returned values

Name	Description
name	Configuration stanza name
integrationKey	Duo integration key for Splunk. Must be of size = 20.
secretKey	Shared secret key between Splunk and Duo.
apiHostname	Duo REST API endpoint used by Splunk for multifactor authentication
appSecretKey	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
failOpen	Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to `false`.
timeout	Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.
sslVersions	SSL version to use for accessing the Duo REST API. Defaults to Splunkd `sslVersion`.
cipherSuite	Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd `cipherSuite`.
ecdhCurves	ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd `ecdhCurves`.
sslVerifyServerCert	Boolean indicating if Duo server certificate verification is required. Defaults to `false`.
sslRootCAPath	Full path of the certificate to be used for certificate verification if *sslVerifyServerCert* is `true`.
sslCommonNameToCheck	Common name to verify if *sslVerifyServerCert* is `true`.
sslAltNameToCheck	Alternate name to verify if *sslVerifyServerCert* is `true`.
useClientSSLCompression	Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd `useClientSSLCompression`.

Example request and response

XML Request

```
admin:changeme -X GET https://localhost:8089/services/admin/Duo-MFA
```

XML Response

```
 <title>Duo-MFA</title>
  <id>https://localhost:8089/services/admin/Duo-MFA</id>
  <updated>2016-07-26T11:05:14-07:00</updated>
  <generator build="321df14f2b1047b51259ee2d4eeacb4184dc6679" version="20160720"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/Duo-MFA/_new" rel="create"/>
  <link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>duo-mfa</title>
    <id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
    <updated>2016-07-26T11:05:14-07:00</updated>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
        <s:key name="appSecretKey">$1$cQdFd4+XlOrAfgBgQEwe+VevD/MOOfFTIA4vwoaFnCX0V0TO8ZsCsKQ=</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="failOpen">0</s:key>
        <s:key name="integrationKey">$1$RHhrEPy965XhV3kSQmB/zyf6IZV/</s:key>
        <s:key name="secretKey">$1$A3t8AvuwwoDzSgUgB1x50FesOpd0ZKBWaHR5xY6uqWeaB02vsuFh4KQ=</s:key>
        <s:key name="sslCommonNameToCheck">*.duosecurity.com</s:key>
        <s:key
name="sslRootCAPath">/home/mkandaswamy/git/splunkApp/etc/auth/DigiCertHighAssuranceEVRootCA.pem</s:key>
        <s:key name="sslVerifyServerCert">true</s:key>
        <s:key name="sslVersions">tls1.2</s:key>
        <s:key name="timeout">5</s:key>
        <s:key name="useClientSSLCompression">true</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create a Duo Multifactor configuration.

Request parameters

Name	Type	Description
name	String	**Required**. Configuration stanza name
integrationKey	See description	**Required**. Duo integration key for Splunk. Must be of size = 20.
secretKey	See description	**Required**. Shared secret key between Splunk and Duo.
apiHostname	See description	**Required**. Duo REST API endpoint used by Splunk for multifactor authentication
appSecretKey	See description	**Required**. Splunk application specific secret key. Must be a random generated hex of length 40 or more.
failOpen	Boolean	Optional. Indicates whether Splunk should bypass the Duo service if it is unavailable. Defaults to `false`.
timeout	Positive integer	Optional. Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to `15` seconds.
sslVersions	See description	Optional. SSL version to use for accessing the Duo REST API. Defaults to Splunkd `sslVersion`.
cipherSuite	See description	Optional. Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd `cipherSuite`.
ecdhCurves	See description	Optional. ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd `ecdhCurves`.
sslVerifyServerCert	Boolean	Optional. Indicates if Duo server certificate verification is required. Defaults to `false`. If set to `true`, provide a *sslRootCAPath* to ensure successful certificate validation.
sslRootCAPath	See description	Optional. Full path of the certificate to be used for certificate verification. If *sslVerifyServerCert* is `true`, this path must be provided to ensure successful certificate validation.
sslCommonNameToCheck	See description	Optional. Common name to verify if *sslVerifyServerCert* is `true`.
sslAltNameToCheck	See description	Optional. Alternate name to verify if *sslVerifyServerCert* is `true`.
useClientSSLCompression	See description	Optional. Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd `useClientSSLCompression`.

Returned values

Name	Description
name	Configuration stanza name
integrationKey	Duo integration key for Splunk. Must be of size = 20.

Name	Description
secretKey	Shared secret key between Splunk and Duo.
apiHostname	Duo REST API endpoint used by Splunk for multifactor authentication
appSecretKey	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
failOpen	Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to `false`.
timeout	Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to `15` seconds.
sslVersions	SSL version to use for accessing the Duo REST API. Defaults to Splunkd `sslVersion`.
cipherSuite	Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd `cipherSuite`.
ecdhCurves	ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd `ecdhCurves`.
sslVerifyServerCert	Boolean that indicates if Duo server certificate verification is required. Defaults to `false`. If set to `true`, provide a *sslRootCAPath* to ensure successful certificate validation.
sslRootCAPath	Full path of the certificate to be used for certificate verification. If *sslVerifyServerCert* is `true`, this path must be provided to ensure successful certificate validation.
sslCommonNameToCheck	Common name to verify if *sslVerifyServerCert* is `true`.
sslAltNameToCheck	Alternate name to verify if *sslVerifyServerCert* is `true`.
useClientSSLCompression	Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd `useClientSSLCompression`.

Example request and response

XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/admin/Duo-MFA/duo-mfa -d
integrationKey=DIOXYOKGDJNK4JRRT0KT -d secretKey=DABZXYbRVW2yqvTM6fPVMkbgxBna0HTuYa9XuCQ2 -d
appSecretKey=56a15e48ec796f3d6ee2763b088f8ca77109692c -d apiHostname=api-cc7a8eab.duosecurity.com -d
failOpen=false -d timeout=10 -d sslVersions=tls1.2 -d sslCommonNameToCheck=*.duosecurity.com -d
useClientSSLCompression=true -d sslVerifyServerCert=true -d
sslRootCAPath=/home/user1/git/example/splunk/etc/auth/DigiCertHighAssuranceEVRootCA.pem
```

XML Response

```
   <title>Duo-MFA</title>
  <id>https://localhost:8089/services/admin/Duo-MFA</id>
  <updated>2016-09-21T14:54:43-07:00</updated>
  <generator build="3fe21d2159a8" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/Duo-MFA/_new" rel="create"/>
  <link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>duo-mfa</title>
    <id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
    <updated>2016-09-21T14:54:43-07:00</updated>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
        <s:key name="appSecretKey">****************************************</s:key>
        <s:key name="cipherSuite">TLSv1+HIGH:TLSv1.2+HIGH:@STRENGTH</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="failOpen">0</s:key>
        <s:key name="integrationKey">$1$W0/LVm4ziyz2U1HZEP8Xzn8WWRa1</s:key>
        <s:key name="secretKey">****************************************</s:key>
        <s:key name="sslCommonNameToCheck">*.duosecurity.com</s:key>
        <s:key
name="sslRootCAPath">/home/user1/git/example/splunk/etc/auth/DigiCertHighAssuranceEVRootCA.pem</s:key>
        <s:key name="sslVerifyServerCert">true</s:key>
        <s:key name="sslVersions">tls1.2</s:key>
        <s:key name="timeout">10</s:key>
        <s:key name="useClientSSLCompression">true</s:key>
      </s:dict>
    </content>
  </entry>
```

admin/Duo-MFA/{name}

Access and manage the `{name}` Duo Multifactor configuration.

Authentication and Authorization

Requires the `change_authentication` capability.

GET

List the `{name}` Duo Multifactor configuration settings.

Request parameters

None

Returned values

Name	Description
name	Configuration stanza name
integrationKey	Duo integration key for Splunk. Must be of size = 20.
secretKey	Shared secret key between Splunk and Duo.
apiHostname	Duo REST API endpoint used by Splunk for multifactor authentication
appSecretKey	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
failOpen	Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to `false`.
timeout	Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.
sslVersions	SSL version to use for accessing the Duo REST API. Defaults to Splunkd `sslVersion`.
cipherSuite	Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd `cipherSuite`.
ecdhCurves	ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd `ecdhCurves`.
sslVerifyServerCert	Boolean indicating if Duo server certificate verification is required. Defaults to `false`.
sslRootCAPath	Full path of the certificate to be used for certificate verification if *sslVerifyServerCert* is `true`.
sslCommonNameToCheck	Common name to verify if *sslVerifyServerCert* is `true`.
sslAltNameToCheck	Alternate name to verify if *sslVerifyServerCert* is `true`.
useClientSSLCompression	Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd `useClientSSLCompression`.

Example request and response

XML Request

```
admin:changeme -X GET https://localhost:8089/services/admin/Duo-MFA
```

XML Response

```
<title>Duo-MFA</title>
 <id>https://localhost:8089/services/admin/Duo-MFA</id>
 <updated>2016-07-26T11:05:14-07:00</updated>
 <generator build="321df14f2b1047b51259ee2d4eeacb4184dc6679" version="20160720"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/admin/Duo-MFA/_new" rel="create"/>
 <link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>duo-mfa</title>
   <id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
   <updated>2016-07-26T11:05:14-07:00</updated>
   <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
   <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
   <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
       <s:key name="appSecretKey">$1$cQdFd4+XlOrAfgBgQEwe+VevD/MOOfFTIA4vwoaFnCX0V0TO8ZsCsKQ=</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">system</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">0</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="failOpen">0</s:key>
       <s:key name="integrationKey">$1$RHhrEPy965XhV3kSQmB/zyf6IZV/</s:key>
       <s:key name="secretKey">$1$A3t8AvuwwoDzSgUgB1x50FesOpd0ZKBWaHR5xY6uqWeaB02vsuFh4KQ=</s:key>
       <s:key name="sslCommonNameToCheck">*.duosecurity.com</s:key>
```

```
        <s:key
name="sslRootCAPath">/home/mkandaswamy/git/splunkApp/etc/auth/DigiCertHighAssuranceEVRootCA.pem</s:key>
        <s:key name="sslVerifyServerCert">true</s:key>
        <s:key name="sslVersions">tls1.2</s:key>
        <s:key name="timeout">5</s:key>
        <s:key name="useClientSSLCompression">true</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update the `{name}` Duo Multifactor configuration.

Request parameters

Name	Type	Description
name	String	Configuration stanza name
integrationKey	See description	Duo integration key for Splunk. Must be of size = 20.
secretKey	See description	Shared secret key between Splunk and Duo.
apiHostname	See description	Duo REST API endpoint used by Splunk for multifactor authentication
appSecretKey	See description	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
failOpen	Boolean	Indicates whether Splunk should bypass the Duo service if it is unavailable. Defaults to `false`.
timeout	Positive integer	Optional. Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to `15` seconds.
sslVersions	See description	Optional. SSL version to use for accessing the Duo REST API. Defaults to Splunkd `sslVersion`.
cipherSuite	See description	Optional. Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd `cipherSuite`.
ecdhCurves	See description	Optional. ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd `ecdhCurves`.
sslVerifyServerCert	Boolean	Optional. Indicates if Duo server certificate verification is required. Defaults to `false`. If set to `true`, provide a *sslRootCAPath* to ensure successful certificate validation.
sslRootCAPath	See description	Optional. Full path of the certificate to be used for certificate verification. If *sslVerifyServerCert* is `true`, this path must be provided to ensure successful certificate validation.
sslCommonNameToCheck	See description	Optional. Common name to verify if *sslVerifyServerCert* is `true`.
sslAltNameToCheck	See description	Optional. Alternate name to verify if *sslVerifyServerCert* is `true`.
useClientSSLCompression	See description	Optional. Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd `useClientSSLCompression`.

Returned values

Name	Description
name	Configuration stanza name
integrationKey	Duo integration key for Splunk. Must be of size = 20.
secretKey	Shared secret key between Splunk and Duo.
apiHostname	Duo REST API endpoint used by Splunk for multifactor authentication
appSecretKey	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
failOpen	Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to `false`.
timeout	Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to `15` seconds.
sslVersions	SSL version to use for accessing the Duo REST API. Defaults to Splunkd `sslVersion`.
cipherSuite	Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd `cipherSuite`.
ecdhCurves	ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd `ecdhCurves`.
sslVerifyServerCert	Boolean that indicates if Duo server certificate verification is required. Defaults to `false`. If set to `true`, provide a *sslRootCAPath* to ensure successful certificate validation.
sslRootCAPath	Full path of the certificate to be used for certificate verification. If *sslVerifyServerCert* is `true`, this path must be provided to ensure successful certificate validation.
sslCommonNameToCheck	Common name to verify if *sslVerifyServerCert* is `true`.
sslAltNameToCheck	Alternate name to verify if *sslVerifyServerCert* is `true`.
useClientSSLCompression	Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd `useClientSSLCompression`.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/Duo-MFA/duo-mfa -d failOpen=0
```

XML Response

```
<title>Duo-MFA</title>
 <id>https://localhost:8089/services/admin/Duo-MFA</id>
 <updated>2016-07-26T11:03:58-07:00</updated>
 <generator build="321d123f2b1047b51259ee2d4eeacb4184dc6679" version="20160720"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/admin/Duo-MFA/_new" rel="create"/>
 <link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>duo-mfa</title>
   <id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
   <updated>2016-07-26T11:03:58-07:00</updated>
   <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
```

```
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
    <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
        <s:key name="appSecretKey">$1$cQdFd4+XlOrAfgBgQEwe+VevD/MOOfFTIA4vwoaFnCX0123TO8ZsCsKQ=</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="failOpen">0</s:key>
        <s:key name="integrationKey">$1$RHhrEPy123XhV3kSQmB/zyf6IZV/</s:key>
        <s:key name="secretKey">$1$A3t8AvuwwoDzSgUgB1x50FesOpd0123WaHR5xY6uqWeaB02vsuFh4KQ=</s:key>
        <s:key name="sslCommonNameToCheck">*.duosecurity.com</s:key>
        <s:key
name="sslRootCAPath">/home/user/git/splunkApp/etc/auth/DigiCertHighAssuranceEVRootCA.pem</s:key>
        <s:key name="sslVerifyServerCert">true</s:key>
        <s:key name="sslVersions">tls1.2</s:key>
        <s:key name="timeout">5</s:key>
        <s:key name="useClientSSLCompression">true</s:key>
      </s:dict>
    </content>
  </entry>
```

DELETE

Delete the `{name}` Duo Multifactor configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme -X DELETE https://localhost:8089/services/admin/Duo-MFA/duo-mfa
```

XML Response

```
...
  <title>Duo-MFA</title>
  <id>https://localhost:8089/services/admin/Duo-MFA</id>
  <updated>2016-07-26T11:06:00-07:00</updated>
  <generator build="321df14f2b1047b51259ee2d4eeacb4184dc6679" version="20160720"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/Duo-MFA/_new" rel="create"/>
  <link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="WARN">No active Duo MFA configuration to list.</s:msg>
  </s:messages>
```

RSA multifactor authentication REST API usage details

Splunk Enterprise users can configure RSA user authentication using the REST API.

You can use the RSA multifactor authentication REST API to configure RSA authentication and to verify that the authentication is configured correctly.

- To configure multifactor authentication for Splunk Web, you use the `/services/admin/Rsa-MFA` endpoint. To enable CLI and management port, set the parameter `enableMfaAuthRest` to true.
- To verify the authentication, you use the `/services/admin/Rsa-MFA-config-verify/` endpoint.

Authentication and Authorization

Requires the `change_authentication` capability.

To learn more about using RSA multifactor authentication, see About multifactor authentication with RSA Authentication Manager in *Securing Splunk Enterprise*.

admin/Rsa-MFA

Configure RSA multifactor authentication.

GET

List the RSA Authentication Manager configuration settings.

Request parameters
None

Returned values

Name	Description
name	Configuration stanza name
authManagerUrl	URL of REST endpoint of RSA Authentication Manager.
accessKey	Access key needed by Splunk to communicate with RSA Authentication Manager. Note that this value is hidden output.
clientId	Agent name created on RSA Authentication Manager is clientId.
failOpen	If true, allow login in case authentication server is unavailable.
timeout	It determines the connection timeout in seconds for the outbound HTTPS connection.
messageOnError	Message that will be shown to user in case of login failure.
enableMfaAuthRest	If true, enable authentication of REST calls.
caCertBundlePayload	SSL certificate chain return by RSA server.
replicateCertificates	If enabled, RSA certificate files are replicated across search head cluster setup.

Example request and response

XML Request

```
curl -k -u admin:changeme -X GET https://ronnie.sv.splunk.com:8130/services/admin/Rsa-MFA/rsa-mfa
```

XML Response

```
...
<title>Rsa-MFA</title>

  <id>https://ronnie.sv.splunk.com:8130/services/admin/Rsa-MFA</id>

  <updated>2018-04-03T12:42:27-07:00</updated>

  <generator build="80906e769c378b3c090160fc090717553dd4e8ef" version="20180331"/>

  <author>

    <name>Splunk</name>

  </author>
```

```
<link href="/services/admin/Rsa-MFA/_new" rel="create"/>
<link href="/services/admin/Rsa-MFA/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>rsa-mfa</title>
  <id>https://ronnie.sv.splunk.com:8130/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="list"/>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="edit"/>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="remove"/>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="accessKey">****************************************</s:key>
      <s:key name="authManagerCertPath">etc/auth/rsa-2fa/cert.pem</s:key>
      <s:key name="authManagerUrl">https://qa-rsaam-002.sv.splunk.com:5555</s:key>
      <s:key name="clientId">ronnie.splunk.com</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="enableMfaAuthRest">false</s:key>
      <s:key name="failOpen">1</s:key>
      <s:key name="messageOnError">Please_contact_admin</s:key>
      <s:key name="timeout">10</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Edit the RSA Authentication Manager configuration.

Request parameters

Name	Type	Description
name	String	Required. Name of RSA configuration stanza
authManagerUrl	String	Required. URL of REST endpoint of RSA Authentication Manager.
accessKey	String	Required. Access key needed by Splunk to communicate with RSA Authentication Manager.
clientId	String	Required. Agent name created on RSA Authentication Manager is clientId.
failOpen	Boolean	Optional. If true, allow login in case authentication server is unavailable.
timeout	Integer	Optional. It determines the connection timeout in seconds for the outbound HTTPS connection.
messageOnError	String	Optional. Message that will be shown to user in case of login failure.
enableMfaAuthRest	Boolean	Optional. If true, enable authentication of REST calls.
caCertBundlePayload	String	Required. SSL certificate chain return by RSA server.
replicateCertificates	Boolean	If enabled, RSA certificate files will be replicated across search head cluster setup.

Returned values

Name	Description
name	Configuration stanza name
authManagerUrl	URL of REST endpoint of RSA Authentication Manager.
accessKey	Access key needed by Splunk to communicate with RSA Authentication Manager. Note that this value is hidden output.
clientId	Agent name created on RSA Authentication Manager is clientId.
failOpen	If true, allow login in case authentication server is unavailable.
timeout	It determines the connection timeout in seconds for the outbound HTTPS connection.
messageOnError	Message that will be shown to user in case of login failure.
enableMfaAuthRest	If true, enable authentication of REST calls.
caCertBundlePayload	SSL certificate chain return by RSA server.
replicateCertificates	If enabled, RSA certificate files will be replicated across search head cluster setup.

Example request and response

XML Request

```
curl -k -u admin:Splunk_123 -X POST https://localhost:8092/services/admin/Rsa-MFA -d name=rsa-mfa  -d
timeout=10 -d failOpen=true -d authManagerUrl=https://rsa-auth-manager.company.com:5555 -d
 accessKey=sdrf23ri90jn00i -d  clientId=linux-vm -d  messageOnError=Please_contact_admin -d
caCertBundlePayload=-----BEGIN%20CERTIFICATE----
-%0AMIIF8jCCBNqgAwIBAgIQDmTF%2B8I2reFLFyrrQceMsDANBgkqhkiG9w0BAQsFADBw%0AMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlna
```

```
UNlcnQgSW5jMRkwFwYDVQQLExB3%0Ad3cuZGlnaWNlcnQuY29tMS8wLQYDVQQDEyZEaWdpQ2VydCBTSEEyIEhpZ2ggQXNz%0AdXJhbmNlIFNlc
nZlciBDQTAeFw0xNTExMDMwMDAwMDBaFw0xODExMjgxMjAwMDBa%0AMIGlMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEUMBIG
A1UEBxML%0ATG9zIEFuZ2VsZXMxPDA6BgNVBAoTM0ludGVybmV0IENvcnBvcmF0aW9uIGZvciBB%0Ac3NpZ25lZCBOYW1lcyBhbmQgTnVtYmVy
czETMBEGA1UECxMKVGVjaG5vbG9neTEY%0AMBYGA1UEAxMPd3d3LmV4YW1wbGUub3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A%0AMIIBCgKC
AQEAs0CWL2FjPiXBl61lRfvvE0KzLJmG9LWAC3bcBjgsH6NiVVo2dt6u%0AXfzi5bTm7F3K7srfUBYkLO78mraM9qizrHoIeyofrV%2Fn%2BpZ
ZJauQsPjCPxMEJnRo%0AD8Z4KpWKX0LyDu1SputoI4nlQ%2FhtEhtiQnuoBfNZxF7WxcxGwEsZuS1KcXIkHl5V%0ARJOreKFHTaXcB1qcZ%2FQ
RaBIv0yhxvK1yBTwWddT4cli6GfHcCe3xGMaSL328Fgs3%0AjYrvG29PueB6VJi%2FtbbPu6qTfwp%2FH1brqdjh29U52Bhb0fJkM9DWxCP%2F
Cattcc7a%0Az8EXnCO%2BLK8vkhw%2FkAiJWPKx4RBvgy73nwIDAQABo4ICUDCCAkwwHwYDVR0jBBgw%0AFoAUUWj%2FkK8CB3U8zNllZGKiEr
hZcjswHQYDVR0OBBYEFKZPYB4fLdHn8SOgKpUW%0A5Oia6m5IMIGBBgNVHREEejB4gg93d3cuZXhhbXBsZS5vcmeCC2V4YW1wbGUuY29t%0Agg
tleGFtcGxlLmVkdYILZXhhbXBsZS5uZXSCC2V4YW1wbGUub3Jngg93d3cuZXhh%0AbXBsZS5jb22CD3d3dy5leGFtcGxlLmVkdYIPd3d3LmV4Y
W1wbGUubmV0MA4GA1Ud%0ADwEB%2FwQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdQYDVR0f%0ABG4wbDA0oDKgMIYuaHR
0cDovL2NybDMuZGlnaWNlcnQuY29tL3NoYTItaGEtc2Vy%0AdmVyLWc0LmNybDA0oDKgMIYuaHR0cDovL2NybDQuZGlnaWNlcnQuY29tL3NoYT
It%0AaGEtc2VydmVyLWc0LmNybDBMBgNVHSAERTBDMDcGCWCGSAGG%2FWwBATAqMCgGCCsG%0AAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2Vy
dC5jb20vQ1BTMAgGBmeBDAECAjCB%0AgwYIKwYBBQUHAQEEdzB1MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2Vy%0AdC5jb20wTQYI
KwYBBQUHMAKGQWh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9E%0AaWdpQ2VydFNIQTJIaWdoQXNzdXJhbmNlU2VydmVyQ0EuY3J0MAwGA1U
dEwEB%2FwQC%0AMAAwDQYJKoZIhvcNAQELBQADggEBAISomhGn2L0LJn5SJHuyVZ3qMIlRCIdvqe0Q%0A6ls%2BC8ctRwRO3UU3x8q8OH%2B2a
hxlQmpzdC5al4XQzJLiLjiJ2Q1p%2Bhub8MFiMmVP%0APZjb2tZm2ipWVuMRM%2BzgpRVM6nVJ9F3vFfUSHOb4%2FJsEIUvPY%2Bd8%2FKrc%2
BkPQwLvy%0AieqRbcuFjmqfyPmUv1U9QoI4TQikpw7TZU0zYZANP4C%2Fgj4Ry48%2FznmUaRvy2kvI%0Al7gRQ21qJTK5suoiYoYNo3J9T%2B
pXPGU7Lydz%2FHwW%2Bw0DpArtAaukI8aNX4ohFUKS%0AwDSiIIWIWJiJGbEeIO0TIFwEVWTOnbNl%2FfaPXpk5IRXicapqiII%3D%0A----
-END%20CERTIFICATE--
```

XML Response

```
...
<title>Rsa-MFA</title>

  <id>https://localhost:8092/services/admin/Rsa-MFA</id>

  <updated>2018-08-09T20:03:01-07:00</updated>

  <generator build="179002a8c333" version="7.2.0"/>

  <author>

    <name>Splunk</name>

  </author>

  <link href="/services/admin/Rsa-MFA/_new" rel="create"/>

  <link href="/services/admin/Rsa-MFA/_acl" rel="_acl"/>

  <opensearch:totalResults>1</opensearch:totalResults>

  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>

  <opensearch:startIndex>0</opensearch:startIndex>

  <s:messages/>

  <entry>

    <title>rsa-mfa</title>

    <id>https://localhost:8092/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa</id>

    <updated>1969-12-31T16:00:00-08:00</updated>

    <link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="alternate"/>

    <author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="list"/>
<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="edit"/>
<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="remove"/>
<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:key name="accessKey">****************************************</s:key>
    <s:key name="authManagerUrl">https://rsa-auth-manager.company.com:5555</s:key>
    <s:key name="clientId">linux-vm</s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app">search</s:key>
        <s:key name="can_change_perms">1</s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_share_app">1</s:key>
        <s:key name="can_share_global">1</s:key>
        <s:key name="can_share_user">0</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">1</s:key>
        <s:key name="owner">nobody</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
```

```
                <s:item>admin</s:item>
                <s:item>power</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">1</s:key>
        <s:key name="sharing">app</s:key>
      </s:dict>
    </s:key>
    <s:key name="eai:appName">search</s:key>
    <s:key name="eai:userName">admin</s:key>
    <s:key name="enableMfaAuthRest">false</s:key>
    <s:key name="failOpen">1</s:key>
    <s:key name="messageOnError">Please_contact_admin</s:key>
    <s:key name="replicateCertificates">true</s:key>
    <s:key name="sslRootCAPath">$SPLUNK_HOME/etc/auth/rsa-2fa/cert.pem</s:key>
    <s:key name="timeout">10</s:key>
  </s:dict>
</content>
</entry>
```

DELETE

Delete the RSA Authentication Manager configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme -X DELETE https://ronnie.sv.splunk.com:8130/services/admin/Rsa-MFA/rsa-mfa
```

XML Response

```
...
 <title>Rsa-MFA</title>

  <id>https://ronnie.sv.splunk.com:8130/services/admin/Rsa-MFA</id>

  <updated>2018-04-03T12:42:27-07:00</updated>

  <generator build="80906e769c378b3c090160fc090717553dd4e8ef" version="20180331"/>

  <author>

    <name>Splunk</name>

  </author>

  <link href="/services/admin/Rsa-MFA/_new" rel="create"/>

  <link href="/services/admin/Rsa-MFA/_acl" rel="_acl"/>

  <opensearch:totalResults>1</opensearch:totalResults>

  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>

  <opensearch:startIndex>0</opensearch:startIndex>

  <s:messages/>

  <entry>

    <title>rsa-mfa</title>

    <id>https://ronnie.sv.splunk.com:8130/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa</id>

    <updated>1969-12-31T16:00:00-08:00</updated>

    <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="alternate"/>

    <author>

      <name>nobody</name>

    </author>

    <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="list"/>

    <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="edit"/>

    <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="remove"/>

    <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa/disable" rel="disable"/>

    <content type="text/xml">

      <s:dict>

        <s:key name="accessKey">****************************************</s:key>
```

```
<s:key name="authManagerCertPath">etc/auth/rsa-2fa/cert.pem</s:key>
<s:key name="authManagerUrl">https://qa-rsaam-002.sv.splunk.com:5555</s:key>
<s:key name="clientId">ronnie.splunk.com</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">system</s:key>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">0</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">nobody</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">1</s:key>
    <s:key name="sharing">system</s:key>
  </s:dict>
```

```
        </s:key>

        <s:key name="enableMfaAuthRest">false</s:key>

        <s:key name="failOpen">1</s:key>

        <s:key name="messageOnError">Please_contact_admin</s:key>

        <s:key name="timeout">10</s:key>

      </s:dict>

    </content>

  </entry>
```

admin/Rsa-MFA-config-verify/<rsa-stanza-name>

Verify RSA multifactor authentication.

POST

Verify the RSA mutifactor authentication.

Request parameters

Name	Type	Description
username'	String	Optional. RSA username.
passcode	String	Optional. RSA passcode consists of PIN followed by tokencode.

Returned values

Information on whether RSA configuration is valid or not.

Example request and response

XML Request

```
curl -k -u user1:Splunk_123 -X POST https://localhost:8201//services/admin/Rsa-MFA-config-verify/rsa-mfa
```

XML Response

```
...
 <title>Rsa-MFA-config-verify</title>

  <id>https://localhost:8201/services/admin/Rsa-MFA-config-verify</id>

  <updated>2018-06-15T22:46:35-07:00</updated>

  <generator build="e23985b8ecacbe6a245c427b75ec77906439d540" version="20180614"/>
  <author>

    <name>Splunk</name>

  </author>
  <link href="/services/admin/Rsa-MFA-config-verify/_acl" rel="_acl"/>

  <opensearch:totalResults>0</opensearch:totalResults>

  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>

  <opensearch:startIndex>0</opensearch:startIndex>

  <s:messages>

    <s:msg type="INFO">Config verification successful</s:msg>

  </s:messages>
```

LDAP REST API usage details

Splunk Enterprise users can configure LDAP user authentication using the REST API. If you are using Splunk Cloud Platform, contact Support for assistance with setting up LDAP authentication.

LDAP user authentication lets you specify configurations, user groups, and group to role mappings to manage permissions in your Splunk deployment.

You can use the LDAP REST API for the following LDAP management tasks.

- Configure an LDAP strategy for a server in your deployment.
- Map LDAP groups to user roles in a server to manage group permissions.
- Enable or disable an LDAP strategy.

To learn more about using LDAP authentication, see Set up user authentication with LDAP in *Securing Splunk Enterprise*.

admin/LDAP-groups

`https://<host>:<mPort>/services/admin/LDAP-groups`
Access and update LDAP group to role mappings.

Authentication and authorization
Requires the `change_authentication` capability for access.

GET

Access LDAP group mappings.

Request parameters

If you are passing in a strategy name with an LDAP group name, they must be comma separated.

Name	Description
strategy	LDAP strategy name
LDAPgroup	LDAP group name

Returned values

For each group, the following values are returned in the response.

Name	Description
roles	Roles mapped to this group
strategy	Strategy name
type	Group type
users	List of users in this group

Example request and response

```
curl -u admin:changeme -X GET -k https://localhost:8089/services/admin/LDAP-groups/

...
  <title>LDAP-groups</title>
  <id>https://localhost:8089/services/admin/LDAP-groups</id>
  <updated>2016-11-10T13:04:02-08:00</updated>
  <generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/LDAP-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>20</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Abc123-Admin</title>
    <id>https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin</id>
    <updated>2016-11-10T13:04:02-08:00</updated>
    <link href="/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin" rel="list"/>
    <link href="/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list/>
        </s:key>
        <s:key name="strategy">ActiveDirectory_New</s:key>
        <s:key name="type">static</s:key>
        <s:key name="users">
          <s:list>
            <s:item>CN=Abc123 CI,OU=Abc123,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:item>
            <s:item>CN=Test 1 User,OU=Abc123,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:item>
            <s:item>CN=Test 2. User,OU=Abc123,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create an LDAP group.

Request parameters

Append the group name to the `LDAP-groups/` endpoint. Pass in a strategy name using comma separation. For example, this POST creates the `ActiveDirectory_New` strategy and specifies the `Abc123` group name.

```
  curl -k -u admin:password -X POST
  https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New,Abc123-Admin -d roles=user
```

Name	Description
strategy	**Required**. LDAP strategy name
LDAPgroup	**Required**. LDAP group name

Returned values

Name	Description
roles	Roles mapped to this group.
strategy	Strategy name
type	Group type
users	List of users in this group.

Name	Description

Example request and response

```
curl -k -u admin:password -X POST
https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New,Abc123-Admin -d roles=user
```

```
.
.
.
    <title>Abc123-Admin</title>
    <id>https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin</id>
    <updated>2016-11-10T13:07:28-08:00</updated>
    <link href="/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin" rel="list"/>
    <link href="/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>user</s:item>
          </s:list>
        </s:key>
        <s:key name="strategy">ActiveDirectory_New</s:key>
        <s:key name="type">static</s:key>
        <s:key name="users">
          <s:list>
```

```
            <s:item>CN=Abc123 CI,OU=Abc123,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:item>
            <s:item>CN=Test 1 User,OU=Abc123,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:item>
            <s:item>CN=Test 2. User,OU=Abc123,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
.
.
.
```

authentication/providers/LDAP

`https://<host>:<mPort>/services/authentication/providers/LDAP`

Access or create LDAP authentication strategies on a server in your deployment.

Authentication and authorization

Requires the `change_authentication` capability for access.

GET

Access LDAP configurations strategies.

Request parameters

Name	Description
strategy	Name of LDAP configuration strategy

Returned values

The response lists LDAP strategy settings.

See LDAP settings in `authentication.conf` for strategy settings information.

Example request and response

```
curl -k -u admin:password https://localhost:8089/services/authentication/providers/LDAP/

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>providers/LDAP</title>
  <id>https://localhost:8089/services/authentication/providers/LDAP</id>
  <updated>2016-11-09T16:14:07-08:00</updated>
  <generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authentication/providers/LDAP/_new" rel="create"/>
  <link href="/services/authentication/providers/LDAP/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

```
<entry>
  <title>my_strategy</title>
  <id>https://localhost:8089/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy</id>
  <updated>2016-11-09T16:14:07-08:00</updated>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="list"/>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="SSLEnabled">0</s:key>
      <s:key name="anonymous_referrals">1</s:key>
      <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
      <s:key name="bindDNpassword">********</s:key>
      <s:key name="charset">utf8</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="emailAttribute">mail</s:key>
      <s:key name="groupBaseDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
      <s:key name="groupMappingAttribute">dn</s:key>
      <s:key name="groupMemberAttribute">sn</s:key>
      <s:key name="groupNameAttribute">sn</s:key>
      <s:key name="host">1.1.1.1</s:key>
      <s:key name="nestedGroups">0</s:key>
      <s:key name="network_timeout">20</s:key>
      <s:key name="order">1</s:key>
      <s:key name="port">389</s:key>
      <s:key name="realNameAttribute">sn</s:key>
      <s:key name="sizelimit">1000</s:key>
      <s:key name="timelimit">15</s:key>
      <s:key name="userBaseDN">OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
      <s:key name="userNameAttribute">sn</s:key>
    </s:dict>
  </content>
  </entry>
</feed>
```

POST

Create an LDAP strategy.

Usage details
Use the following endpoints to enable or disable an LDAP strategy after you create it.

- `services/authentication/providers/LDAP/{LDAP_strategy_name}/enable`
- `services/authentication/providers/LDAP/{LDAP_strategy_name}/disable`

Request parameters
See LDAP settings in `authentication.conf` for required and optional settings information.

Returned values
None.

Example request and response

```
curl -k u admin:password -X POST https://localhost:8089/services/authentication/providers/LDAP/ -d
name=my_strategy -d groupBaseDN="CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com" -d
groupMemberAttribute=sn -d groupNameAttribute=sn -d host=1.1.1.1 -d realNameAttribute=sn -d
userBaseDN="OU=SAML Test,DC=qa,DC=ab2008e2,DC=com" -d userNameAttribute=sn -d bindDN="CN=Saml user2,OU=SAML
Test,DC=qa,DC=ad2008r2,DC=com" -d bindDNpassword=password
```

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>providers/LDAP</title>
  <id>https://localhost:8089/services/authentication/providers/LDAP</id>
  <updated>2016-11-09T16:20:14-08:00</updated>
  <generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authentication/providers/LDAP/_new" rel="create"/>
  <link href="/services/authentication/providers/LDAP/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Successfully performed a bind to the LDAP server</s:msg>
    <s:msg type="WARN">Failed to find the email attribute 'mail' in a returned user entry.</s:msg>
  </s:messages>
  <entry>
    <title>my_strategy</title>
    <id>https://localhost:8089/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy</id>
    <updated>2016-11-09T16:20:14-08:00</updated>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="list"/>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="SSLEnabled">0</s:key>
        <s:key name="anonymous_referrals">1</s:key>
        <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
        <s:key name="bindDNpassword">********</s:key>
        <s:key name="charset">utf8</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="emailAttribute">mail</s:key>
        <s:key name="groupBaseDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
        <s:key name="groupMappingAttribute">dn</s:key>
        <s:key name="groupMemberAttribute">sn</s:key>
        <s:key name="groupNameAttribute">sn</s:key>
        <s:key name="host">1.1.1.1</s:key>
        <s:key name="nestedGroups">0</s:key>
        <s:key name="network_timeout">20</s:key>
        <s:key name="order">1</s:key>
        <s:key name="port">389</s:key>
        <s:key name="realNameAttribute">sn</s:key>
        <s:key name="sizelimit">1000</s:key>
        <s:key name="timelimit">15</s:key>
        <s:key name="userBaseDN">OU=SAML Test,DC=qa,DC=ab2008e2,DC=com</s:key>
        <s:key name="userNameAttribute">sn</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

authentication/providers/LDAP/{LDAP_strategy_name}

`https://<host>:<mPort>/services/authentication/providers/LDAP/{LDAP_strategy_name}`

Access, update, or delete the `{LDAP_strategy_name}` strategy.

Authentication and authorization
Requires the `change_authentication` capability for access.

POST

Update an existing LDAP strategy.

Request parameters and returned values
See LDAP settings in `authentication.conf` for strategy settings information.

Example request and response

```
curl -k -u admin:password -X POST https://localhost:8089/services/authentication/providers/LDAP/my_strategy
-d port=390
```

```
  <entry>
    <title>my_strategy</title>
    <id>https://localhost:8089/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy</id>
    <updated>2016-11-09T16:14:07-08:00</updated>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="list"/>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/>
    <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="SSLEnabled">0</s:key>
        <s:key name="anonymous_referrals">1</s:key>
        <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
        <s:key name="bindDNpassword">********</s:key>
        <s:key name="charset">utf8</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="emailAttribute">mail</s:key>
        <s:key name="groupBaseDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
        <s:key name="groupMappingAttribute">dn</s:key>
        <s:key name="groupMemberAttribute">sn</s:key>
        <s:key name="groupNameAttribute">sn</s:key>
        <s:key name="host">1.1.1.1</s:key>
        <s:key name="nestedGroups">0</s:key>
        <s:key name="network_timeout">20</s:key>
        <s:key name="order">1</s:key>
        <s:key name="port">390</s:key>
        <s:key name="realNameAttribute">sn</s:key>
        <s:key name="sizelimit">1000</s:key>
        <s:key name="timelimit">15</s:key>
        <s:key name="userBaseDN">OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
        <s:key name="userNameAttribute">sn</s:key>
      </s:dict>
    </content>
  </entry>
.
.
.
```

DELETE

Delete an existing LDAP strategy.

Request parameters

None

Returned values

None

Example request and response

```
curl -k -u admin:password -X DELETE
https://localhost:8089/services/authentication/providers/LDAP/my_strategy

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>providers/LDAP</title>
  <id>https://ronnie:8132/services/authentication/providers/LDAP</id>
  <updated>2016-11-09T16:18:37-08:00</updated>
  <generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authentication/providers/LDAP/_new" rel="create"/>
  <link href="/services/authentication/providers/LDAP/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

authentication/providers/LDAP/{LDAP_strategy_name}/enable

```
https://<host>:<mPort>/services/authentication/providers/LDAP/{LDAP_strategy_name}/enable
```

POST

Enable the `{LDAP_strategy_name}` LDAP strategy.

Request parameters
None

Returned values
None

Example request

```
curl -k -u admin:password -X POST
https://localhost:8089/services/authentication/providers/LDAP/my_strategy/enable
```

authentication/providers/LDAP/{LDAP_strategy_name}/disable

```
https://<host>:<mPort>/services/authentication/providers/LDAP/{LDAP_strategy_name}/disable
```

POST

Disable the `{LDAP_strategy_name}` LDAP strategy.

Request parameters
None

Returned values
None

Example request

```
curl -k -u admin:password -X POST
https://localhost:8089/services/authentication/providers/LDAP/my_strategy/disable
```

admin/metrics-reload/_reload

```
https://<host>:<mPort>/services/admin/metrics-reload/_reload
```

Use this endpoint to reload the metrics processor after updating a metrics-related configuration.

POST

Reload the metrics processor.

Example request and response

Request

```
curl -k -u admin:changeme \https://localhost:8089/services/admin/metrics-reload/_reload
```

Response

```
...
<title>metrics-reload</title>
  <id>https://<localhost>:<mport>/services/admin/metrics-reload</id>
  <updated>2017-08-08T23:33:13+00:00</updated>
  <generator build="eb729684699b" version="7.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/metrics-reload/_reload" rel="_reload"/>
  <link href="/services/admin/metrics-reload/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

ProxySSO REST API usage details

SSO mode must be enabled before you can configure ProxySSO. If you are creating a new ProxySSO configuration for the first time, follow these steps.

1. Locate the `web.conf` file in the `etc/system/local` directory.
2. Make the following additions to the `[settings]` stanza of `web.conf` file. If the file does not already exist in this location, create a new file called `web.conf` and add only the `[settings]` stanza name and the following settings to it.
   ```
   [settings]
   SSOMode = strict
   trustedIP = <IP_address>
   remoteUser = <remote user>
   remoteGroups = <remote group>
   tools.proxy.on = False
   allowSsoWithoutChangingServerConf = 1
   ```
3. Restart the Splunk deployment after updating `web.conf`.
4. Use the admin/ProxySSO-auth/{proxy_name}/enable endpoint to enable the configuration that you are creating.
5. Use the admin/ProxySSO-auth endpoint to add the new configuration.
6. (Optional) Use the `services/admin/auth-services` endpoint to verify that the `active_authmodule` is set to `ProxySSO`.

admin/ProxySSO-auth

`https://<host>:<mPort>/services/admin/ProxySSO-auth`

Access or create a ProxySSO configuration.

GET

Review existing ProxySSO configurations.

Request parameters

None.

Returned values

For each configuration the following values are returned.

Name	Description
defaultRoleIfMissing	Name of default role to use if no mapping is found.
blacklistedUsers	Comma separated list of blacklisted users.
blacklistedAutoMappedRoles	Comma separated list of blacklisted roles.
disabled	Boolean value indicating whether the configuration is disabled. `0` indicates that the configuration is enabled.
title	Configuration name

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth
```

XML Response

```
...
  <title>ProxySSO-auth</title>
  <id>https://localhost:8089/services/admin/ProxySSO-auth</id>
  <updated>2016-08-31T15:57:42-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>my_proxy</title>
    <id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
    <updated>2016-08-31T15:57:42-07:00</updated>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="alternate"/>
    <author>
```

```
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="list"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="edit"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="remove"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="blacklistedAutoMappedRoles">role1</s:key>
        <s:key name="blacklistedUsers"></s:key>
        <s:key name="defaultRoleIfMissing"></s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>

...
```

POST

Add a new ProxySSO configuration.

Usage details

Changes are written to the app context.

Request parameters

Name	Type	Description

Name	Type	Description
name	String	**Required.** New ProxySSO configuration name
defaultRoleIfMissing	Role name	Specify a default role to use if no mapping is found.
blacklistedUsers	Comma separated list	Specify blacklisted users.
blacklistedAutoMappedRoles	Comma separated list	Specify blacklisted roles.

Returned values

Name	Description
defaultRoleIfMissing	Name of default role to use if no mapping is found.
blacklistedUsers	Comma separated list of blacklisted users.
blacklistedAutoMappedRoles	Comma separated list of blacklisted roles.
disabled	Boolean value indicating whether the configuration is disabled. `0` indicates that the configuration is enabled.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth -d name=my_proxy
```

XML Response

```
...
<title>ProxySSO-auth</title>
  <id>https://wimpy:7102/services/admin/ProxySSO-auth</id>
  <updated>2016-08-31T14:53:42-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>my_proxy</title>
    <id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
    <updated>2016-08-31T14:53:42-07:00</updated>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="list"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="edit"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="remove"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="blacklistedAutoMappedRoles"></s:key>
        <s:key name="blacklistedUsers"></s:key>
        <s:key name="defaultRoleIfMissing"></s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
...
```

admin/ProxySSO-auth/{proxy_name}

`https://<host>:<mPort>/services/admin/ProxySSO-auth/{proxy_name}`

Access, update, or delete the `{proxy_name}` configuration.

GET

Access configuration details.

Request parameters

None

Returned values

Name	Description
defaultRoleIfMissing	Name of default role to use if no mapping is found.
blacklistedUsers	Comma separated list of blacklisted users.
blacklistedAutoMappedRoles	Comma separated list of blacklisted roles.
disabled	

Name	Description
	Boolean value indicating whether the configuration is disabled. `0` indicates that the configuration is enabled.
title	Configuration name

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy
```

XML Response

```
<title>ProxySSO-auth</title>
  <id>https://localhost:8089/services/admin/ProxySSO-auth</id>
      ...
  <entry>
    <title>my_proxy</title>
    <id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
    <updated>2016-08-31T16:09:38-07:00</updated>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="list"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="edit"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="remove"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="blacklistedAutoMappedRoles">role1</s:key>
        <s:key name="blacklistedUsers"></s:key>
        <s:key name="defaultRoleIfMissing"></s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>blacklistedAutoMappedRoles</s:item>
                <s:item>blacklistedUsers</s:item>
                <s:item>defaultRoleIfMissing</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update a configuration.

Changes are written to the app context.

Request parameters

Name	Type	Description
name	String	**Required.** New ProxySSO configuration name
defaultRoleIfMissing	Role name	Specify a default role to use if no mapping is found.
blacklistedUsers	Comma separated list	Specify blacklisted users.
blacklistedAutoMappedRoles	Comma separated list	Specify blacklisted roles.

Returned values

Name	Description
defaultRoleIfMissing	Name of default role to use if no mapping is found.
blacklistedUsers	Comma separated list of blacklisted users.
blacklistedAutoMappedRoles	Comma separated list of blacklisted roles.
disabled	Boolean value indicating whether the configuration is disabled. `0` indicates that the configuration is enabled.
title	Configuration name

Name	Description

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy -d
blacklistedAutoMappedRoles=role2,role3
```

XML Response

```
...
 <title>ProxySSO-auth</title>
  <id>https://localhost:8089/services/admin/ProxySSO-auth</id>
  <updated>2016-08-31T16:19:07-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>my_proxy</title>
    <id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
    <updated>2016-08-31T16:19:07-07:00</updated>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="list"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="edit"/>
    <link href="/services/admin/ProxySSO-auth/my_proxy" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="blacklistedAutoMappedRoles">role2,role3</s:key>
        <s:key name="blacklistedUsers"></s:key>
        <s:key name="defaultRoleIfMissing"></s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
```

```
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

DELETE

Delete a configuration.

Changes are written to the app context.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme -X DELETE https://localhost:8089/services/admin/ProxySSO-auth/my_proxy
```

XML Response

admin/ProxySSO-auth/{proxy_name}/disable

```
https://<host>:<mPort>/services/admin/ProxySSO-auth/{proxy_name}/disable
```

Disable the `{proxy_name}` configuration.

GET

Disable the `{proxy_name}` configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy/disable
```

XML Response

```
...
  <title>ProxySSO-auth</title>
  <id>https://localhost:8089/services/admin/ProxySSO-auth</id>
  <updated>2016-08-31T16:43:46-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
...
```

admin/ProxySSO-auth/{proxy_name}/enable

```
https://<host>:<mPort>/services/admin/ProxySSO-auth/{proxy_name}/enable
```

Use a GET request to create and enable the `{proxy_name}` authentication setting. Changes are made in the default app context.

GET

Enable the `{proxy_name}` configuration.

Usage details
For new configurations, specify a new `{proxy_name}`. After enabling the configuration, use the same `{proxy_name}` in the POST to `admin/ProxySSO-auth` to add the configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy/enable
```

XML Response

```
  <title>ProxySSO-auth</title>
  <id>https://wimpy:7102/services/admin/ProxySSO-auth</id>
  <updated>2016-08-31T16:44:05-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

admin/ProxySSO-groups

```
https://<host>:<mPort>/services/admin/ProxySSO-groups
```

Access or create role to group ProxySSO mappings.

Authentication and authorization

Requires the `change_authentication` capability.

GET

Access ProxySSO role to group mappings.

Request parameters

None

Returned values

For each group returned, lists the `roles` assigned to it.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-groups
```

XML Response

```
...
  <title>ProxySSO-groups</title>
  <id>https://localhost:8089/services/admin/ProxySSO-groups</id>
```

```
     ...
  <entry>
    <title>group1</title>
    <id>https://localhost:8089/services/admin/ProxySSO-groups/group1</id>
    <updated>2016-08-31T17:03:46-07:00</updated>
    <link href="/services/admin/ProxySSO-groups/group1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-groups/group1" rel="list"/>
    <link href="/services/admin/ProxySSO-groups/group1" rel="edit"/>
    <link href="/services/admin/ProxySSO-groups/group1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
...
```

POST

Create a new mapping.

Changes are written to the app context.

Request parameters

Name	Type	Description
roles	User role name	Specify roles to map to the group that you are creating. Use a separate `roles` parameter for each role added.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changed -X POST https://localhost:8089/services/admin/ProxySSO-groups/group1 -d roles=power
```

XML Response

```
...
  <title>ProxySSO-groups</title>
  <id>https://localhost:8089/services/admin/ProxySSO-groups</id>
  <updated>2016-08-31T17:01:20-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-groups/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
 ...
```

admin/ProxySSO-groups/{group_name}

```
https://<host>:<mPort>/services/admin/ProxySSO-groups/{group_name}
```

Access, create, and manage role to group mappings.

Authentication and authorization

Requires the `change_authentication` capability.

GET

Access role mappings for the `{group_name}` group.

Request parameters

None

Returned values

Name	Description

roles	Roles mapped to this group.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-groups/group2
```

XML Response

```
  <title>ProxySSO-groups</title>
  <id>https://wimpy:7102/services/admin/ProxySSO-groups</id>
   ...
  <entry>
    <title>group2</title>
    <id>https://localhost:8089/services/admin/ProxySSO-groups/group2</id>
    <updated>2016-08-31T17:25:01-07:00</updated>
    <link href="/services/admin/ProxySSO-groups/group2" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-groups/group2" rel="list"/>
    <link href="/services/admin/ProxySSO-groups/group2" rel="edit"/>
    <link href="/services/admin/ProxySSO-groups/group2" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>roles</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>user</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
...
```

POST

Create a new `{group_name}` mapping or update an existing one.

Changes are written to the app context.

Request parameters
If you are creating a new group, specify the new group name in the URL.

Name	Type	Description
roles	User role name	Specify roles to map to the group that you are creating or updating. Use a separate `roles` parameter for each role added.

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changed -X POST https://localhost:8089/services/admin/ProxySSO-groups/group1 -d roles=power
```

XML Response

```
...
  <title>ProxySSO-groups</title>
  <id>https://localhost:8089/services/admin/ProxySSO-groups</id>
  <updated>2016-08-31T17:01:20-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
```

```
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-groups/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
 ...
```

DELETE

Delete the `{group_name}` group mapping.

Changes are written to the app context.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changed -X DELETE https://localhost:8089/services/admin/ProxySSO-groups/group2
```

XML Response

```
  <title>ProxySSO-groups</title>
  <id>https://localhost:8089/services/admin/ProxySSO-groups</id>
  <updated>2016-08-31T17:42:39-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-groups/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

admin/ProxySSO-user-role-map

`https://<host>:<mPort>/services/admin/ProxySSO-user-role-map`
Access or create a user to role mapping.

Authentication and authorization
Requires the `edit_user` capability.

GET

Access user to role mappings

Request parameters
None

Returned values

Name	Description
roles	Roles mapped to the user
title	User name

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-user-role-map
```

XML Response

```
 ...
  <title>ProxySSO-user-role-map</title>
  <id>https://localhost:8089/services/admin/ProxySSO-user-role-map</id>
    ...
  <entry>
    <title>user1</title>
    <id>https://localhost:8089/services/admin/ProxySSO-user-role-map/user1</id>
    <updated>2016-08-31T18:00:28-07:00</updated>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="list"/>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
...
```

POST

Create a user to role mapping.

Changes are written to the `etc/system/local` directory.

Note: User to role mappings cannot be updated.

Request parameters

Name	Type	Description
name	User name	Specify a user to map to specific roles
roles	User role name	Specify a role to map to the user. Use a separate `roles` parameter for each role that you are mapping.

Returned values

None

XML Request

```
curl -k -u admin:changed -X POST https://localhost:8089/services/admin/ProxySSO-user-role-map -d name=user1
 -d roles=power
```

XML Response

```
  <title>ProxySSO-user-role-map</title>
  <id>https://wimpy:7102/services/admin/ProxySSO-user-role-map</id>
   ...
  <entry>
    <title>user1</title>
    <id>https://wimpy:7102/services/admin/ProxySSO-user-role-map/user1</id>
    <updated>2016-08-31T17:57:53-07:00</updated>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="list"/>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
...
```

admin/ProxySSO-user-role-map/{user_name}

`https://<host>:<mPort>/services/admin/ProxySSO-user-role-map/{user_name}`

Access or delete a user to role mapping.

Authentication and authorization

Requires the `edit_user` capability.

GET

Access role mappings for the `{user_name}` user.

Request parameters

None

Returned values

Name	Description
roles	Roles mapped to the `{user_name}` user.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-user-role-map/user1
```

XML Response

```
  <title>ProxySSO-user-role-map</title>
  <id>https://wimpy:7102/services/admin/ProxySSO-user-role-map</id>
  <updated>2016-08-31T18:13:01-07:00</updated>
  ...
  <entry>
    <title>user1</title>
    <id>https://localhost:8089/services/admin/ProxySSO-user-role-map/user1</id>
    <updated>2016-08-31T18:13:01-07:00</updated>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="list"/>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
```

```
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
...
```

DELETE

Delete the `{user_name}` user to role mapping.

Changes are written to the `etc/system/local` directory.

Request parameters
None

Returned values
The response lists remaining user to role mappings.

Example request and response

XML Request

```
curl -k -u admin:changed -X DELETE https://localhost:8089/services/admin/ProxySSO-user-role-map/user2
```

XML Response

```
 <title>ProxySSO-user-role-map</title>
  <id>https://localhost:8089/services/admin/ProxySSO-user-role-map</id>
   ...
  <entry>
    <title>user1</title>
    <id>https://localhost:8089/services/admin/ProxySSO-user-role-map/user1</id>
    <updated>2016-08-31T18:11:02-07:00</updated>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="list"/>
    <link href="/services/admin/ProxySSO-user-role-map/user1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

SAML REST API usage details

Splunk Enterprise users can configure SAML authentication for single sign-on (SSO). If you are using Splunk Cloud Platform, contact Support to request assistance.

You can use the REST API to make the following SAML configurations.

- Manage group and user role mappings.
- Access service and identity provider information.
- Replicate SAML IdP certificates across a search head cluster.

For more information on using SAML for SSO, see Authentication using single sign-on with SAML in *Securing Splunk Enterprise*. You can also review the SAML settings stanza in authentication.conf in the *Admin Manual*.

admin/replicate-SAML-certs

`https://<host>:<mPort>/services/admin/replicate-SAML-certs`
Replicate SAML IdP certificates across a search head cluster.

Note: This endpoint is only available for use on search head clustered deployments with KV Store enabled.

Authentication and authorization
Requires the `change_authentication` capability for access.

POST

Usage details
After editing SAML IdP certificate files in `$SPLUNK_HOME/etc/auth/idpCerts` on one node in the cluster, you can POST to `/replicate-SAML-certs` to replicate the certificates across the cluster. This can be useful if there is an error in the certificate files from `/SAML-idp-metadata` and you need to edit them manually.

There are no request parameters or returned values.

admin/SAML-groups

`https://<host>:<mPort>/services/admin/SAML-groups`
Manage external groups in an IdP response to internal Splunk roles.

Authentication and authorization
Requires `change_authentication` capability for all operations.

GET

Access internal roles for this external group.

Request parameters
None.

Response keys

Name	Description
roles	Corresponding internal role for the external group.

Example request and response

XML Request

```
curl -k -u admin:password https://localhost:8089/services/admin/SAML-groups
```

XML Response

```
<title>SAML-groups</title>
  <id>https://localhost:8089/services/admin/SAML-groups</id>
  <updated>2015-11-07T18:00:05-08:00</updated>
  <generator build="05ee6658a12a17d11f47076b544" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-groups/_new" rel="create"/>
  <link href="/services/admin/SAML-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>4</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>admin</title>
    <id>https://localhost:8089/services/admin/SAML-groups/admin</id>
    <updated>2015-11-07T18:00:05-08:00</updated>
    <link href="/services/admin/SAML-groups/admin" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-groups/admin" rel="list"/>
    <link href="/services/admin/SAML-groups/admin" rel="edit"/>
    <link href="/services/admin/SAML-groups/admin" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="roles">
        <s:list>
          <s:item>sc_admin</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>employee</title>
  <id>https://localhost:8089/services/admin/SAML-groups/employee</id>
  <updated>2015-11-07T18:00:05-08:00</updated>
  <link href="/services/admin/SAML-groups/employee" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/admin/SAML-groups/employee" rel="list"/>
  <link href="/services/admin/SAML-groups/employee" rel="edit"/>
  <link href="/services/admin/SAML-groups/employee" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>_spl_cloud</s:item>
                  <s:item>_spl_cloud_user</s:item>
                  <s:item>admin</s:item>
                  <s:item>spl_cloud_user</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>_spl_cloud</s:item>
                  <s:item>_spl_cloud_user</s:item>
                  <s:item>admin</s:item>
                  <s:item>spl_cloud_user</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="roles">
        <s:list>
          <s:item>user</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>power admin</title>
  <id>https://localhost:8089/services/admin/SAML-groups/power%20admin</id>
  <updated>2015-11-07T18:00:05-08:00</updated>
  <link href="/services/admin/SAML-groups/power%20admin" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/admin/SAML-groups/power%20admin" rel="list"/>
  <link href="/services/admin/SAML-groups/power%20admin" rel="edit"/>
  <link href="/services/admin/SAML-groups/power%20admin" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>_spl_cloud</s:item>
                  <s:item>_spl_cloud_user</s:item>
                  <s:item>admin</s:item>
                  <s:item>spl_cloud_user</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>_spl_cloud</s:item>
                  <s:item>_spl_cloud_user</s:item>
                  <s:item>admin</s:item>
                  <s:item>spl_cloud_user</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="roles">
        <s:list>
          <s:item>power</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>user admin</title>
  <id>https://localhost:8089/services/admin/SAML-groups/user%20admin</id>
  <updated>2015-11-07T18:00:05-08:00</updated>
  <link href="/services/admin/SAML-groups/user%20admin" rel="alternate"/>
```

```
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-groups/user%20admin" rel="list"/>
    <link href="/services/admin/SAML-groups/user%20admin" rel="edit"/>
    <link href="/services/admin/SAML-groups/user%20admin" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Convert an external group to internal roles.

Request parameters

Name	Type	Description

name	String	External group name.
roles	String	Equivalent internal role for the group.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/admin/SAML-groups -d name=Splunk -d roles=user
```

XML Response

```
  <title>SAML-groups</title>
  <id>https://localhost:8089/services/admin/SAML-groups</id>
  <updated>2015-11-07T18:04:56-08:00</updated>
  <generator build="05ee6658a1d11f47076b549133a47050ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-groups/_new" rel="create"/>
  <link href="/services/admin/SAML-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

admin/SAML-groups/{group_name}

`https://<host>:<mPort>/services/admin/SAML-groups/{group_name}`

Delete the `{group_name}` group.

Authentication and authorization

Requires `change_authentication` capability for all operations.

DELETE

Delete the `{group_name}` particular group.

Request parameters

None

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:password --request DELETE https://localhost:8089/services/admin/SAML-groups/group_to_delete
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>SAML-groups</title>
  <id>https://localhost:8089/services/admin/SAML-groups</id>
  <updated>2015-11-07T18:04:25-08:00</updated>
  <generator build="05ee6658a12a17d11f47133a47050ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-groups/_new" rel="create"/>
  <link href="/services/admin/SAML-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

admin/SAML-idp-metadata

`https://<host>:<mPort>/services/admin/SAML-idp-metadata`
Access IdP SAML metadata attributes.

Authentication and authorization

Requires `change_authentication` capability for all operations.

GET

Access SAML user and role information for saved searches.

Request parameters

Name	Type	Description
idpMetadataFile	File path. See description.	Full path of the metadata file location. File should be local to splunkd server.

Response keys

Name	Description
idpMetadataPayload	SAML IdP metadata in XML format.

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/admin/SAML-idp-metadata
```

XML Response

```
<title>SAML-idp-metadata</title>
  <id>https://localhost:8089/services/admin/SAML-idp-metadata</id>
  <updated>2015-11-07T18:34:07-08:00</updated>
  <generator build="05ee6658a12a17d11f47076h3453ffdd50ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-idp-metadata/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>idpMetadataPayload</title>
    <id>https://localhost:8089/services/admin/SAML-idp-metadata/idpMetadataPayload</id>
    <updated>2015-11-07T18:34:07-08:00</updated>
    <link href="/services/admin/SAML-idp-metadata/idpMetadataPayload" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-idp-metadata/idpMetadataPayload" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key
name="idpCertificatePayload"><![CDATA[MIIDpjCCAo6gAwIBAgIGAU7gBZ6oMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYDVQQGEwJVUz
ETMBEG
A1UECAwKQ2FsaWZvcrterye444uIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFDASBgNVBAMMC3NwbHVua3Rlc3QxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvQG9rdGEuY29tMB4XDTE1MDczMDE3MzEyMVoXDTQ1MDczMDE3MzIyMVowgZMxCzAJBgNV
BAYTAlnJhbmNpc2NvMQ0wCwYD
VQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEUMBIGA1UEAwwLc3BsdW5rdGVzdDExHDAa
BgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCQS0Zh/PCBRsbHkJhi6RtGSkEzFjPZyPyFr2ND9KysDf4WRgMiklOBdrlM/++BJkqPCTYFbt/L
ZXnVqo7v9wJ538MrTp6o1iBi52zhpDnqAoOIrlSaB0PbbQVd/oz49YbEW6/ThsAMHdIyz3/CSqEM
o6oD7GiQzoGH4jidhx1Gjgmfk2OdkKAnWQDmZGKAMHJQXtjfrUK3y0H5j2tla9iIPLUVDyopzWNa
o8TKw68iWDZs9ZGrwu9ptF4fpjiaslkWp3oyO1FmAencabXMddFZ7HgVziI2TjbExNa+bzS9SUhY
gZlf2meD/ib2ul6HVFKlVM0IJA56qWGImiJRzGj1AgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAC+I
566v40xTMhFjTlF3sRGjbXQDnJGXcuF1GFkAp/IEmdo
7mawu7Z7qcHb2BcQiVViuHY5ON2O/gbz5ggDipc803JMD7dTtFxDthfZgvN1tE/nPNgx2QAKCADw
FkhYwAf6R7zV1VvyRfUzmbbl6V9JZh7Mju0vFsVJUsGhsAqJfZWQ+QckedB/NIpr9OxBu4IYgMZ4
gbV4yQ+FaICBh/vpqrtp5KmIIp63gXuV+Lh71NW0dj8oty3JpJmjZEdwXPjBKp5Xx94KHiA7Esyh
+7Zk/NK0PJTvlTrsyk+UIeSJZE473SdxI7A=]]></s:key>
        <s:key name="protocol_endpoints">
          <s:dict>
            <s:key
name="idpSLOUrl">https://test.example.com/app/example/exk4nkqqsypk32FMF0h7/slo/saml</s:key>
            <s:key
name="idpSSOUrl">https://test.example.com/app/example/exk4nkqqsypk32FMF0h7/sso/saml</s:key>
          </s:dict>
        </s:key>
        <s:key name="signAuthnRequest">1</s:key>
      </s:dict>
    </content>
  </entry>
```

admin/SAML-sp-metadata

`https://<host>:<mPort>/services/admin/SAML-sp-metadata`

Access service provider SAML metadata attributes.

Authentication and authorization

Requires `change_authentication` capability for all operations.

GET

Access SAML metadata attributes.

Request parameters

None.

Response keys

Name	Description
spMetadataPayload	SAML service provider metadata in XML format.

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/admin/SAML-sp-metadata
```

XML Response

```
  <title>SAML-sp-metadata</title>
  <id>https://localhost:8089/services/admin/SAML-sp-metadata</id>
  <updated>2015-12-16T13:47:39-08:00</updated>
  <generator build="d48f9f793521" version="6.4.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-sp-metadata/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>spMetadata</title>
    <id>https://localhost:8089/services/admin/SAML-sp-metadata/spMetadata</id>
    <updated>2015-12-16T13:47:39-08:00</updated>
    <link href="/services/admin/SAML-sp-metadata/spMetadata" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-sp-metadata/spMetadata" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="spMetadata"><![CDATA[<md:EntityDescriptor entityID="splunkEntityId"
```

```
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
 <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
 AuthnRequestsSigned="true"  WantAssertionsSigned="true">  <md:KeyDescriptor>  <ds:KeyInfo>  <ds:X509Data>
 <ds:X509Certificate>
MIICLTCCAZYCCQDCCiSo4+bLSzANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDzANBgNVBAoM
BlNwbHVuazEXMBUGA1UEAwwOU3BsdW5rQ29tbW9uQ0ExITAfBgkqhkiG9w0BCQEW
EnN1cHBvcnRAc3BsdW5rLmNvbTAeFw0xNTA3MjgxNjMzNDNaFw0xODA3MjcxNjMz
NDNaMDcxIDAeBgNVBAMMF1NwbHVerTRer55ZlckRlZmF1bHRDZXJ0MRMwEQYDVQQK
DApTcGx1bmtVc2VyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmxUfArn3l
Pxn24lBl1pWDFg5VCB/f8IS7MlEFPJiepioAli+yE7exlzD0wRniw2Akiyg1Kbt9
zNe1z9Dxi1fEOailFaV5ryENabYgYJFJonZKWucNvWzde50Cn4fm1nNqVSZOH90F
9zTGCD7Kkem0hIqx506TI2C2dKP+cJWeWwIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
ADy75DKIegJo2ALOZsckvrllqGZ2+g/xBupuRBDBSRp9vs3VqN+wB39uDtMzXlZ1
u0J5OhPVMdqO0RJuYzZmFpAhCX4hFfsNeazfFzSK/DQCURvfYG4pZit3P8gJ6uDv
3OxcDGUorMNlGRRO61UAkrLUywE44MMs1jgidDw2QlMY
</ds:X509Certificate>  </ds:X509Data>  </ds:KeyInfo>  </md:KeyDescriptor>
 <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:SingleLogoutService  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="http://example-unix-58667/saml/logout"  index="0">  </md:SingleLogoutService>
 <md:AssertionConsumerService  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="http://example-unix-58667/saml/acs"  index="0">  </md:AssertionConsumerService>
 </md:SPSSODescriptor> </md:EntityDescriptor> ]]></s:key>
      </s:dict>
    </content>
  </entry>
```

admin/SAML-user-role-map

`https://<host>:<mPort>/services/admin/SAML-user-role-map`

Access or create SAML user and role information for saved searches if your IdP does not support Attribute Query Requests. To delete a username, see `admin/SAML-user-role-map/{name}`.

Authentication and authorization

Requires `edit_user` capability for all operations.

GET

Access SAML user and role information for saved searches.

Request parameters

None.

Response keys

Name	Description
name	SAML username for running saved searches.
roles	Assigned roles for this user.

Example request and response

XML Request

```
curl -k -u admin:password https://localhost:8089/services/admin/SAML-user-role-map
```

XML Response

```
  <title>SAML-user-role-map</title>
  <id>https://localhost:8089/services/admin/SAML-user-role-map</id>
  <updated>2015-11-07T17:34:12-08:00</updated>
  <generator build="05ee6658a12a17d11f47076b549133a47050ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-user-role-map/_new" rel="create"/>
  <link href="/services/admin/SAML-user-role-map/_acl" rel="_acl"/>
  <opensearch:totalResults>3</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>samluser001@example.com</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser001%40example.com</id>
    <updated>2015-11-07T17:34:12-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="email">samluser001@example.com</s:key>
        <s:key name="realname">Firstname Lastname001</s:key>
        <s:key name="roles">
          <s:list>
            <s:item>sc_admin</s:item>
            <s:item>user</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>samluser002@example.com</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser002%40example.com</id>
    <updated>2015-11-07T17:34:12-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      <s:key name="email">samluser002@example.com</s:key>
      <s:key name="realname">Firstname Lastname002</s:key>
      <s:key name="roles">
        <s:list>
          <s:item>power</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>samluser003@example.com</title>
  <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser003%40example.com</id>
  <updated>2015-11-07T17:34:12-08:00</updated>
  <link href="/services/admin/SAML-user-role-map/samluser003%40example.com" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/admin/SAML-user-role-map/samluser003%40example.com" rel="list"/>
  <link href="/services/admin/SAML-user-role-map/samluser003%40example.com" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>_spl_cloud</s:item>
                  <s:item>_spl_cloud_user</s:item>
                  <s:item>admin</s:item>
                  <s:item>sc_admin</s:item>
                  <s:item>spl_cloud_user</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>_spl_cloud</s:item>
                  <s:item>_spl_cloud_user</s:item>
                  <s:item>admin</s:item>
                  <s:item>sc_admin</s:item>
                  <s:item>spl_cloud_user</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="email">samluser003@example.com</s:key>
      <s:key name="realname">Firstname Lastname003</s:key>
      <s:key name="roles">
        <s:list>
          <s:item>user</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update SAML user and role information for saved searches.

Request parameters

Name	Type	Description
name	String	SAML username for running saved searches.
roles	String	Assigned roles for this user.

Response keys

Name	Description
name	SAML username for running saved searches.
roles	Assigned roles for this user.

Example request and response

XML Request

```
curl -k -u admin:password https://localhost:8089/services/admin/SAML-user-role-map -d
name=samluser004@example.foo -d roles=user
```

XML Response

```
 <title>SAML-user-role-map</title>
  <id>https://localhost:8089/services/admin/SAML-user-role-map</id>
  <updated>2015-11-07T17:45:54-08:00</updated>
  <generator build="05ee6658a12a17d11f47076b549133a47050ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-user-role-map/_new" rel="create"/>
  <link href="/services/admin/SAML-user-role-map/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>samluser004@example.foo</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser004%40example.foo</id>
    <updated>2015-11-07T17:45:54-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser004%40example.foo" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser004%40example.foo" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser004%40example.foo" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>user</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

DELETE

See `admin/SAML-user-role-map/{name}`

admin/SAML-user-role-map/{name}

`https://<host>:<mPort>/services/admin/SAML-user-role-map/{name}`

Delete SAML user and role information for saved searches if your IdP does not support Attribute Query Requests.

Authentication and authorization
Requires `edit_user` capability for all operations.

DELETE

Remove a username from SAML users for saved searches.

Request parameters

None.

Response keys

Name	Description
name	SAML username for running saved searches.
roles	Assigned roles for this user.

Example request and response

XML Request

```
curl -k -u admin:password --request DELETE
https://localhost:8089/services/admin/SAML-user-role-map/samluser004@example.com
```

XML Response

```
 <title>SAML-user-role-map</title>
  <id>https://localhost:8089/services/admin/SAML-user-role-map</id>
  <updated>2015-11-07T17:46:26-08:00</updated>
  <generator build="05ee6658a12a17d11f47076b549133a47050ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-user-role-map/_new" rel="create"/>
  <link href="/services/admin/SAML-user-role-map/_acl" rel="_acl"/>
  <opensearch:totalResults>3</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>samluser001@example.com</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser001%40example.com</id>
    <updated>2015-11-07T17:46:26-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
```

```
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>sc_admin</s:item>
            <s:item>user</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>samluser002@example.com</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser002%40example.com</id>
    <updated>2015-11-07T17:46:26-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>power</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>samluser003@example.com</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser003%40example.com</id>
    <updated>2015-11-07T17:46:26-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser003%40example.com" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser003%40example.com" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser003%40example.com" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>_spl_cloud</s:item>
                    <s:item>_spl_cloud_user</s:item>
                    <s:item>admin</s:item>
                    <s:item>sc_admin</s:item>
                    <s:item>spl_cloud_user</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="roles">
          <s:list>
            <s:item>user</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

authentication/providers/SAML

`https://<host>:<mPort>/services/authentication/providers/SAML`
Access and create SAML configurations.

Authentication and authorization
Requires `change_authentication` capability for all operations.

GET

Access SAML configurations.

Request parameters
None.

Response keys

Name	Description
allowSslCompression	Indicates whether ssl data compression is enabled.
assertionConsumerServiceUrl	Endpoint where SAML assertions are posted by the IdP.
attributeAliasMail	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.

Name	Description
attributeAliasRealName	Specifies which SAML attribute maps to 'realName'. Defaults to `realName`.
attributeAliasRole	Specifies which SAML attribute maps to `role`. Defaults to `role`.
attributeQueryRequestSigned	Indicates whether Attribute Queries should be signed.
attributeQueryResponseSigned	Indicates whether Attribute Query responses should be signed.
attributeQuerySoapPassword	Credentials for making Attribute Query using SOAP over HTTP.
attributeQuerySoapUsername	Credentials for making Attribute Query using SOAP over HTTP.
attributeQueryTTL	ttl (time to live) for the Attribute Query credentials cache.
blacklistedAutoMappedRoles	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
blacklistedUsers	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.
caCertFile	File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem
cipherSuite	Ciphersuite for making Attribute Queries using ssl. For example, `TLSv1+HIGH:@STRENGTH`.
defaultRoleIfMissing	Default role to use if no role is returned in a SAML response.
ecdhCurves	EC curves for ECDH/ECDHE key exchange - ssl setting.
entityId	Unique id preconfigured by the IdP.
errorUrL	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or Splunk deployment.
errorUrlLabel	Label or title of the content to which errorUrl points. Defaults to `Click here to resolve SAML error.`.
fqdn	Load balancer url.
idpAttributeQueryUrl	IdP attribute query url where SAML attribute queries are sent.
idpCertPath	Path for IdP certificate.
idpSLOUrl	IdP sso url where SAML SSO requests are sent.
idpSSOUrl	IdP SSO url where SAML SLO requests are sent.
maxAttributeQueryQueueSize	Maximum number of Attribute jobs to queue.
maxAttributeQueryThreads	Maximum number of threads for asynchronous Attribute Queries.
name	Configuration stanza name.

nameIdFormat	Specifies how subject is identified in SAML Assertion. Defaults to
	`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
	Override it when using Azure AD as an IDP and set it to
	`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`

redirectAfterLogoutToUrl	Redirect URL after user logout If no SLO URL is configured.
redirectPort	Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The `assertionconsumerServiceUrl` in the `AuthNRequest` uses the set port instead of the splunkweb port. To prevent any port information being appended to the `assertionConsumerServiceUrl`, set to `0`.

Name	Description
signAuthnRequest	Indicates whether to sign authentication requests.
signatureAlgorithm	Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when *signedAuthnRequest* is set to `true`. Possible values are: • `RSA-SHA1` (default) ♦ corresponds to `http://www.w3.org/2000/09/xmldsig#rsa-sha1` • `RSA-SHA256` ♦ corresponds to `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`
signedAssertion	Indicates whether to sign SAML assertions.
singleLogoutServiceUrl	URL where the IdP posts SAML Single Logout responses.
skipAttributeQueryRequestForUsers	Used in conjunction with `defaultRoleIFMissing`. Indicates whether to skip Attribute Queries for some users.
sloBinding	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.
spCertPath	Service provider certificate path.
sslAltNameToCheck	Alternate name to check in the peer certificate.
sslCommonNameToCheck	Common name to check in the peer certificate.
sslKeysfile	Location of service provider private key.
sslKeysfilePassword	SSL password.
sslVerifyServerCert	Indicates whether to verify peer certificate.
sslVersions	SSL versions.
ssoBinding	Binding used when making a SP-initiated SAML request. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.
uiStatusPage	Splunk Web page for redirecting users in case of errors.

Example request and response

XML Request

```
curl -u admin:pass -k -X GET  https://localhost:8089/services/authentication/providers/SAML
```

XML Response

```
  <title>SAML-auth</title>
  <id>https://localhost:8089/services/authentication/providers/SAML</id>
  <updated>2017-04-10T23:27:22+00:00</updated>
  <generator build="a8914247a786" version="6.5.1612"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authentication/providers/SAML/_new" rel="create"/>
  <link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
```

```
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>saml-test</title>
  <id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
  <updated>2017-04-10T23:27:22+00:00</updated>
  <link href="/services/authentication/providers/SAML/saml-test" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/providers/SAML/saml-test" rel="list"/>
  <link href="/services/authentication/providers/SAML/saml-test" rel="edit"/>
  <link href="/services/authentication/providers/SAML/saml-test" rel="remove"/>
  <link href="/services/authentication/providers/SAML/saml-test/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="allowSslCompression">true</s:key>
      <s:key name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:key>
      <s:key name="attributeQueryRequestSigned">1</s:key>
      <s:key name="attributeQueryResponseSigned">1</s:key>
      <s:key name="attributeQuerySoapPassword">******</s:key>
      <s:key name="attributeQuerySoapUsername">test_ping</s:key>
      <s:key name="attributeQueryTTL">3600</s:key>
      <s:key name="attribute_aliases"/>
      <s:key name="blacklistedAutoMappedRoles">
        <s:list/>
      </s:key>
      <s:key name="blacklistedUsers">
        <s:list/>
      </s:key>
      <s:key name="caCertFile">/opt/splunk/etc/auth/cacert.pem</s:key>
      <s:key name="cipherSuite"></s:key>
      <s:key name="defaultRoleIfMissing"></s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
```

```
        <s:key name="ecdhCurves"></s:key>
        <s:key name="entityId">saml-test-entity</s:key>
        <s:key name="errorUrl"></s:key>
        <s:key name="errorUrlLabel"></s:key>
        <s:key name="fqdn">http://so1</s:key>
        <s:key name="idpCertChains">
          <s:list/>
        </s:key>
        <s:key name="idpCertPath"></s:key>
        <s:key name="maxAttributeQueryQueueSize">100</s:key>
        <s:key name="maxAttributeQueryThreads">2</s:key>
        <s:key name="nameIdFormat"></s:key>
        <s:key name="protocol_endpoints">
          <s:dict>
            <s:key name="idpAttributeQueryUrl">https://saml-idp:9999/idp/attrsvc.ssaml2</s:key>
            <s:key name="idpSLOUrl"></s:key>
            <s:key name="idpSSOUrl">https://saml-idp:9999/idp/SSO.saml2</s:key>
            <s:key name="issuerId"></s:key>
          </s:dict>
        </s:key>
        <s:key name="redirectAfterLogoutToUrl">http://www.splunk.com</s:key>
        <s:key name="redirectPort">12800</s:key>
        <s:key name="replicateCertificates">1</s:key>
        <s:key name="signAuthnRequest">1</s:key>
        <s:key name="signatureAlgorithm">
          <s:dict>
            <s:key name="name">RSA-SHA1</s:key>
            <s:key name="uri">http://www.w3.org/2000/09/xmldsig#rsa-sha1</s:key>
          </s:dict>
        </s:key>
        <s:key name="signedAssertion">1</s:key>
        <s:key name="singleLogoutServiceUrl">http://so1:12800/saml/logout</s:key>
        <s:key name="skipAttributeQueryRequestForUsers">
          <s:list/>
        </s:key>
        <s:key name="sloBinding">HTTPPost</s:key>
        <s:key name="spCertPath">/opt/splunk/etc/auth/server.pem</s:key>
        <s:key name="sslAltNameToCheck"></s:key>
        <s:key name="sslCommonNameToCheck"></s:key>
        <s:key name="sslKeysfile">/opt/splunk/etc/auth/server.pem</s:key>
        <s:key name="sslKeysfilePassword">******</s:key>
        <s:key name="sslVerifyServerCert">false</s:key>
        <s:key name="sslVersions">SSL3,TLS1.0,TLS1.1,TLS1.2</s:key>
        <s:key name="ssoBinding">HTTPPost</s:key>
        <s:key name="uiStatusPage">/account/status</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create a new SAML configuration.

Request parameters

Name	Description
allowSslCompression	Indicates whether ssl data compression is enabled.
attributeAliasMail	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
attributeAliasRealName	Specifies which SAML attribute maps to 'realName'. Defaults to `realName`.

Name	Description
attributeAliasRole	Specifies which SAML attribute maps to `role`. Defaults to `role`.
attributeQueryRequestSigned	Indicates whether Attribute Queries should be signed.
attributeQueryResponseSigned	Indicates whether Attribute Query responses should be signed.
attributeQuerySoapPassword	Credentials for making Attribute Query using SOAP over HTTP.
attributeQuerySoapUsername	Credentials for making Attribute Query using SOAP over HTTP.
attributeQueryTTL	ttl (time to live) for the Attribute Query credentials cache.
blacklistedAutoMappedRoles	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
blacklistedUsers	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.
caCertFile	File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem
cipherSuite	Ciphersuite for making Attribute Queries using ssl. For example, `TLSv1+HIGH:@STRENGTH`.
defaultRoleIfMissing	Default role to use if no role is returned in a SAML response.
ecdhCurves	EC curves for ECDH/ECDHE key exchange - ssl setting.
entityId	**Required**. Unique id preconfigured by the IdP.
errorUrL	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or the Splunk deployment.
errorUrlLabel	Label or title of the content to which errorUrl points. Defaults to `Click here to resolve SAML error.`.
fqdn	Load balancer url.
idpAttributeQueryUrl	IdP attribute query url where SAML attribute queries are sent.
idpCertPath	Path for IdP certificate.
idpMetadataFile	Full path to idpMetadata on disk. Used to retrieve IdP information such as idpSLOUrl, idpSSOUrl, and signing certificate.
idpSLOUrl	IdP sso url where SAML SSO requests are sent.
idpSSOUrl	**Required**. IdP SSO url where SAML SLO requests are sent.
name	**Required**. Configuration stanza name.
nameIdFormat	Specifies how subject is identified in SAML Assertion. Defaults to `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` Override it when using Azure AD as an IDP and set it to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
redirectAfterLogoutToUrl	Redirect URL after user logout If no SLO URL is configured.
redirectPort	Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The `assertionconsumerServiceUrl` in the `AuthNRequest` uses the set port instead of the splunkweb port. To prevent any port information being appended to the `assertionConsumerServiceUrl`, set to `0`.
signAuthnRequest	Indicates whether to sign authentication requests.

Name	Description
signatureAlgorithm	Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when *signedAuthnRequest* is set to `true`. Possible values are: • `RSA-SHA1` (default) ♦ corresponds to `http://www.w3.org/2000/09/xmldsig#rsa-sha1` • `RSA-SHA256` ♦ corresponds to `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`
signedAssertion	Indicates whether to sign SAML assertions.
skipAttributeQueryRequestForUsers	Used in conjunction with `defaultRoleIFMissing`. Indicates whether to skip Attribute Queries for some users.
sloBinding	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.
sslAltNameToCheck	Alternate name to check in the peer certificate.
sslCommonNameToCheck	Common name to check in the peer certificate.
sslKeysfile	Location of service provider private key.
sslKeysfilePassword	SSL password.
sslVerifyServerCert	Indicates whether to verify peer certificate.
sslVersions	SSL versions.
ssoBinding	Binding used when making a SP-initiated SAML request. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.

Response keys

None.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/authentication/providers/SAML -d "name=saml-test"
-d "idpSSOUrl=https://saml-idp:9999/idp/SSO.saml2" -d
"idpAttributeQueryUrl=https://saml-idp:9999/idp/attrsvc.ssaml2" -d "entityId=saml-test-entity" -d
"attributeQuerySoapPassword=splunk" -d "attributeQuerySoapUsername=test_ping"
```

XML Response

```
  <title>SAML-auth</title>
  <id>https://localhost:8089/services/authentication/providers/SAML</id>
  <updated>2017-04-10T23:26:35+00:00</updated>
  <generator build="a8914247a786" version="6.5.1612"/>
  <author>
    <name>Splunk</name>
  </author>
```

```
<link href="/services/authentication/providers/SAML/_new" rel="create"/>
<link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>saml-test</title>
  <id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
  <updated>2017-04-10T23:26:35+00:00</updated>
  <link href="/services/authentication/providers/SAML/saml-test" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/providers/SAML/saml-test" rel="list"/>
  <link href="/services/authentication/providers/SAML/saml-test" rel="edit"/>
  <link href="/services/authentication/providers/SAML/saml-test" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="allowSslCompression">true</s:key>
      <s:key name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:key>
      <s:key name="attributeQueryRequestSigned">1</s:key>
      <s:key name="attributeQueryResponseSigned">1</s:key>
      <s:key name="attributeQuerySoapPassword">******</s:key>
      <s:key name="attributeQuerySoapUsername">test_ping</s:key>
      <s:key name="attributeQueryTTL">3600</s:key>
      <s:key name="attribute_aliases"/>
      <s:key name="blacklistedAutoMappedRoles">
        <s:list/>
      </s:key>
      <s:key name="blacklistedUsers">
        <s:list/>
      </s:key>
      <s:key name="caCertFile">/opt/splunk/etc/auth/cacert.pem</s:key>
      <s:key name="cipherSuite"></s:key>
      <s:key name="defaultRoleIfMissing"></s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="ecdhCurves"></s:key>
      <s:key name="entityId">saml-test-entity</s:key>
      <s:key name="errorUrl"></s:key>
      <s:key name="errorUrlLabel"></s:key>
      <s:key name="fqdn">http://so1</s:key>
      <s:key name="idpCertChains">
        <s:list/>
      </s:key>
      <s:key name="idpCertPath"></s:key>
      <s:key name="maxAttributeQueryQueueSize">100</s:key>
      <s:key name="maxAttributeQueryThreads">2</s:key>
      <s:key name="nameIdFormat"></s:key>
      <s:key name="protocol_endpoints">
        <s:dict>
          <s:key name="idpAttributeQueryUrl">https://saml-idp:9999/idp/attrsvc.ssaml2</s:key>
          <s:key name="idpSLOUrl"></s:key>
          <s:key name="idpSSOUrl">https://saml-idp:9999/idp/SSO.saml2</s:key>
          <s:key name="issuerId"></s:key>
        </s:dict>
      </s:key>
      <s:key name="redirectAfterLogoutToUrl">http://www.splunk.com</s:key>
      <s:key name="redirectPort">12800</s:key>
      <s:key name="replicateCertificates">1</s:key>
      <s:key name="signAuthnRequest">1</s:key>
      <s:key name="signatureAlgorithm">
        <s:dict>
          <s:key name="name">RSA-SHA1</s:key>
          <s:key name="uri">http://www.w3.org/2000/09/xmldsig#rsa-sha1</s:key>
        </s:dict>
      </s:key>
      <s:key name="signedAssertion">1</s:key>
      <s:key name="singleLogoutServiceUrl">http://so1:12800/saml/logout</s:key>
      <s:key name="skipAttributeQueryRequestForUsers">
        <s:list/>
      </s:key>
      <s:key name="sloBinding">HTTPPost</s:key>
      <s:key name="spCertPath">/opt/splunk/etc/auth/server.pem</s:key>
      <s:key name="sslAltNameToCheck"></s:key>
      <s:key name="sslCommonNameToCheck"></s:key>
      <s:key name="sslKeysfile">/opt/splunk/etc/auth/server.pem</s:key>
      <s:key name="sslKeysfilePassword">******</s:key>
      <s:key name="sslVerifyServerCert">false</s:key>
      <s:key name="sslVersions">SSL3,TLS1.0,TLS1.1,TLS1.2</s:key>
      <s:key name="ssoBinding">HTTPPost</s:key>
      <s:key name="uiStatusPage">/account/status</s:key>
    </s:dict>
  </content>
</entry>
```

authentication/providers/SAML/{stanza_name}

```
https://<host>:<mPort>/services/authentication/providers/SAML/{stanza_name}
```

GET

Access a SAML configuration.

Request parameters
None.

Response keys

Name	Description
allowSslCompression	Indicates whether ssl data compression is enabled.
assertionConsumerServiceUrl	Endpoint where SAML assertions are posted by the IdP.
attributeAliasMail	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
attributeAliasRealName	Specifies which SAML attribute maps to 'realName'. Defaults to `realName`.
attributeAliasRole	Specifies which SAML attribute maps to `role`. Defaults to `role`.
attributeQueryRequestSigned	Indicates whether Attribute Queries should be signed.
attributeQueryResponseSigned	Indicates whether Attribute Query responses should be signed.
attributeQuerySoapPassword	Credentials for making Attribute Query using SOAP over HTTP.
attributeQuerySoapUsername	Credentials for making Attribute Query using SOAP over HTTP.
attributeQueryTTL	ttl (time to live) for the Attribute Query credentials cache.
blacklistedAutoMappedRoles	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
blacklistedUsers	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.
caCertFile	File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem
cipherSuite	Ciphersuite for making Attribute Queries using ssl. For example, `TLSv1+HIGH:@STRENGTH`.
defaultRoleIfMissing	Default role to use if no role is returned in a SAML response.
ecdhCurves	EC curves for ECDH/ECDHE key exchange - ssl setting.
entityId	Unique id preconfigured by the IdP.
errorUrL	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or Splunk deployment.
errorUrlLabel	Label or title of the content to which errorUrl points. Defaults to `Click here to resolve SAML error.`.
fqdn	Load balancer url.
idpAttributeQueryUrl	IdP attribute query url where SAML attribute queries are sent.
idpCertPath	Path for IdP certificate.
idpSLOUrl	IdP sso url where SAML SSO requests are sent.
idpSSOUrl	IdP SSO url where SAML SLO requests are sent.
maxAttributeQueryQueueSize	Maximum number of Attribute jobs to queue.
maxAttributeQueryThreads	Maximum number of threads for asynchronous Attribute Queries.

Name	Description
name	Configuration stanza name.
nameIdFormat	Specifies how subject is identified in SAML Assertion. Defaults to `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` Override it when using Azure AD as an IDP and set it to `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
redirectAfterLogoutToUrl	Redirect URL after user logout If no SLO URL is configured.
redirectPort	Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The `assertionconsumerServiceUrl` in the `AuthNRequest` uses the set port instead of the splunkweb port. To prevent any port information being appended to the `assertionConsumerServiceUrl`, set to `0`.
signAuthnRequest	Indicates whether to sign authentication requests.
signatureAlgorithm	Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when *signedAuthnRequest* is set to `true`. Possible values are: • `RSA-SHA1` (default) ♦ corresponds to `http://www.w3.org/2000/09/xmldsig#rsa-sha1` • `RSA-SHA256` ♦ corresponds to `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`
signedAssertion	Indicates whether to sign SAML assertions.
singleLogoutServiceUrl	URL where the IdP posts SAML Single Logout responses.
skipAttributeQueryRequestForUsers	Used in conjunction with `defaultRoleIFMissing`. Indicates whether to skip Attribute Queries for some users.
sloBinding	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.
spCertPath	Service provider certificate path.
sslAltNameToCheck	Alternate name to check in the peer certificate.
sslCommonNameToCheck	Common name to check in the peer certificate.
sslKeysfile	Location of service provider private key.
sslKeysfilePassword	SSL password.
sslVerifyServerCert	Indicates whether to verify peer certificate.
sslVersions	SSL versions.
ssoBinding	Binding used when making a SP-initiated SAML request. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.
uiStatusPage	Splunk Web page for redirecting users in case of errors.

Example request and response

XML Request

```
 curl -k -u admin:password https://localhost:8089/services/authentication/providers/SAML/saml_settings
```

XML Response

```
<title>SAML-auth</title>
  <id>https://localhost:8089/services/authentication/providers/SAML</id>
  <updated>2017-04-10T23:29:58+00:00</updated>
  <generator build="a8914247a786" version="6.5.1612"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authentication/providers/SAML/_new" rel="create"/>
  <link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>saml-test</title>
    <id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
    <updated>2017-04-10T23:29:58+00:00</updated>
    <link href="/services/authentication/providers/SAML/saml-test" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authentication/providers/SAML/saml-test" rel="list"/>
    <link href="/services/authentication/providers/SAML/saml-test" rel="edit"/>
    <link href="/services/authentication/providers/SAML/saml-test" rel="remove"/>
    <link href="/services/authentication/providers/SAML/saml-test/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="allowSslCompression">true</s:key>
        <s:key name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:key>
        <s:key name="attributeQueryRequestSigned">1</s:key>
        <s:key name="attributeQueryResponseSigned">1</s:key>
        <s:key name="attributeQuerySoapPassword">******</s:key>
        <s:key name="attributeQuerySoapUsername">test_ping</s:key>
        <s:key name="attributeQueryTTL">3600</s:key>
        <s:key name="attribute_aliases"/>
        <s:key name="blacklistedAutoMappedRoles">
          <s:list/>
        </s:key>
        <s:key name="blacklistedUsers">
          <s:list/>
        </s:key>
        <s:key name="caCertFile">/opt/splunk/etc/auth/cacert.pem</s:key>
        <s:key name="cipherSuite"></s:key>
        <s:key name="defaultRoleIfMissing"></s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>allowSslCompression</s:item>
                <s:item>attributeAliasMail</s:item>
                <s:item>attributeAliasRealName</s:item>
                <s:item>attributeAliasRole</s:item>
                <s:item>attributeQueryRequestSigned</s:item>
                <s:item>attributeQueryResponseSigned</s:item>
                <s:item>attributeQuerySoapPassword</s:item>
                <s:item>attributeQuerySoapUsername</s:item>
                <s:item>attributeQueryTTL</s:item>
                <s:item>blacklistedAutoMappedRoles</s:item>
                <s:item>blacklistedUsers</s:item>
                <s:item>caCertFile</s:item>
                <s:item>cipherSuite</s:item>
                <s:item>defaultRoleIfMissing</s:item>
                <s:item>ecdhCurveName</s:item>
                <s:item>ecdhCurves</s:item>
                <s:item>entityId</s:item>
                <s:item>errorUrl</s:item>
                <s:item>errorUrlLabel</s:item>
                <s:item>fqdn</s:item>
                <s:item>idpAttributeQueryUrl</s:item>
                <s:item>idpCertChains</s:item>
                <s:item>idpCertPath</s:item>
                <s:item>idpCertificatePayload</s:item>
                <s:item>idpMetadataFile</s:item>
                <s:item>idpMetadataPayload</s:item>
                <s:item>idpSLOUrl</s:item>
                <s:item>idpSSOUrl</s:item>
                <s:item>issuerId</s:item>
                <s:item>nameIdFormat</s:item>
                <s:item>redirectAfterLogoutToUrl</s:item>
                <s:item>redirectPort</s:item>
                <s:item>replicateCertificates</s:item>
                <s:item>signAuthnRequest</s:item>
                <s:item>signatureAlgorithm</s:item>
                <s:item>signedAssertion</s:item>
                <s:item>skipAttributeQueryRequestForUsers</s:item>
                <s:item>sloBinding</s:item>
                <s:item>sslAltNameToCheck</s:item>
                <s:item>sslCommonNameToCheck</s:item>
                <s:item>sslKeysfile</s:item>
                <s:item>sslKeysfilePassword</s:item>
                <s:item>sslVerifyServerCert</s:item>
```

```
              <s:item>sslVersions</s:item>
              <s:item>ssoBinding</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="ecdhCurves"></s:key>
      <s:key name="entityId">saml-test-entity</s:key>
      <s:key name="errorUrl"></s:key>
      <s:key name="errorUrlLabel"></s:key>
      <s:key name="fqdn">http://so1</s:key>
      <s:key name="idpCertChains">
        <s:list/>
      </s:key>
      <s:key name="idpCertPath"></s:key>
      <s:key name="maxAttributeQueryQueueSize">100</s:key>
      <s:key name="maxAttributeQueryThreads">2</s:key>
      <s:key name="nameIdFormat"></s:key>
      <s:key name="protocol_endpoints">
        <s:dict>
          <s:key name="idpAttributeQueryUrl">https://saml-idp:9999/idp/attrsvc.ssaml2</s:key>
          <s:key name="idpSLOUrl"></s:key>
          <s:key name="idpSSOUrl">https://saml-idp:9999/idp/SSO.saml2</s:key>
          <s:key name="issuerId"></s:key>
        </s:dict>
      </s:key>
      <s:key name="redirectAfterLogoutToUrl">http://www.splunk.com</s:key>
      <s:key name="redirectPort">12800</s:key>
      <s:key name="replicateCertificates">1</s:key>
      <s:key name="signAuthnRequest">1</s:key>
      <s:key name="signatureAlgorithm">
        <s:dict>
          <s:key name="name">RSA-SHA1</s:key>
          <s:key name="uri">http://www.w3.org/2000/09/xmldsig#rsa-sha1</s:key>
        </s:dict>
      </s:key>
      <s:key name="signedAssertion">1</s:key>
      <s:key name="singleLogoutServiceUrl">http://so1:12800/saml/logout</s:key>
      <s:key name="skipAttributeQueryRequestForUsers">
        <s:list/>
      </s:key>
      <s:key name="sloBinding">HTTPPost</s:key>
      <s:key name="spCertPath">/opt/splunk/etc/auth/server.pem</s:key>
      <s:key name="sslAltNameToCheck"></s:key>
      <s:key name="sslCommonNameToCheck"></s:key>
      <s:key name="sslKeysfile">/opt/splunk/etc/auth/server.pem</s:key>
      <s:key name="sslKeysfilePassword">******</s:key>
      <s:key name="sslVerifyServerCert">false</s:key>
      <s:key name="sslVersions">SSL3,TLS1.0,TLS1.1,TLS1.2</s:key>
      <s:key name="ssoBinding">HTTPPost</s:key>
      <s:key name="uiStatusPage">/account/status</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update a SAML configuration.

Request parameters

Name	Description
allowSslCompression	Indicates whether ssl data compression is enabled.
attributeAliasMail	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
attributeAliasRealName	Specifies which SAML attribute maps to 'realName'. Defaults to `realName`.
attributeAliasRole	Specifies which SAML attribute maps to `role`. Defaults to `role`.
attributeQueryRequestSigned	Indicates whether Attribute Queries should be signed.
attributeQueryResponseSigned	Indicates whether Attribute Query responses should be signed.
attributeQuerySoapPassword	Credentials for making Attribute Query using SOAP over HTTP.
attributeQuerySoapUsername	Credentials for making Attribute Query using SOAP over HTTP.
attributeQueryTTL	ttl (time to live) for the Attribute Query credentials cache.
blacklistedAutoMappedRoles	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
blacklistedUsers	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.
caCertFile	File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem
cipherSuite	Ciphersuite for making Attribute Queries using ssl. For example, `TLSv1+HIGH:@STRENGTH`.
defaultRoleIfMissing	Default role to use if no role is returned in a SAML response.
ecdhCurves	EC curves for ECDH/ECDHE key exchange - ssl setting.
entityId	**Required**. Unique id preconfigured by the IdP.
errorUrL	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or the Splunk deployment.
errorUrlLabel	Label or title of the content to which errorUrl points. Defaults to `Click here to resolve SAML error.`.
fqdn	Load balancer url.
idpAttributeQueryUrl	IdP attribute query url where SAML attribute queries are sent.
idpCertPath	Path for IdP certificate.
idpSLOUrl	IdP sso url where SAML SSO requests are sent.
idpSSOUrl	**Required**. IdP SSO url where SAML SLO requests are sent.
name	**Required**. Configuration stanza name.

nameIdFormat	Specifies how subject is identified in SAML Assertion. Defaults to
	`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
	Override it when using Azure AD as an IDP and set it to
	`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`

redirectAfterLogoutToUrl	Redirect URL after user logout If no SLO URL is configured.
redirectPort	

Name	Description
	Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The `assertionconsumerServiceUrl` in the `AuthNRequest` uses the set port instead of the splunkweb port. To prevent any port information being appended to the `assertionConsumerServiceUrl`, set to `0`.
signAuthnRequest	Indicates whether to sign authentication requests.
signatureAlgorithm	Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when *signedAuthnRequest* is set to `true`. Possible values are: • `RSA-SHA1` (default) ♦ corresponds to `http://www.w3.org/2000/09/xmldsig#rsa-sha1` • `RSA-SHA256` ♦ corresponds to `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`
signedAssertion	Indicates whether to sign SAML assertions.
skipAttributeQueryRequestForUsers	Used in conjunction with `defaultRoleIFMissing`. Indicates whether to skip Attribute Queries for some users.
sloBinding	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.
sslAltNameToCheck	Alternate name to check in the peer certificate.
sslCommonNameToCheck	Common name to check in the peer certificate.
sslKeysfile	Location of service provider private key.
sslKeysfilePassword	SSL password.
sslVerifyServerCert	Indicates whether to verify peer certificate.
sslVersions	SSL versions.
ssoBinding	Binding used when making a SP-initiated SAML request. Possible values are `HTTPPost` (default) and `HTTPRedirect`. This binding must match the binding configured on the IDP.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/authentication/providers/SAML/saml-test -d
"entityId=someOtherEntityId"
```

XML Response

```
 <title>SAML-auth</title>
  <id>https://localhost:8089/services/authentication/providers/SAML</id>
  <updated>2017-04-10T23:30:41+00:00</updated>
```

```
<generator build="a8914247a786" version="6.5.1612"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/providers/SAML/_new" rel="create"/>
<link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>saml-test</title>
  <id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
  <updated>2017-04-10T23:30:41+00:00</updated>
  <link href="/services/authentication/providers/SAML/saml-test" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/providers/SAML/saml-test" rel="list"/>
  <link href="/services/authentication/providers/SAML/saml-test" rel="edit"/>
  <link href="/services/authentication/providers/SAML/saml-test" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="allowSslCompression">true</s:key>
      <s:key name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:key>
      <s:key name="attributeQueryRequestSigned">1</s:key>
      <s:key name="attributeQueryResponseSigned">1</s:key>
      <s:key name="attributeQuerySoapPassword">******</s:key>
      <s:key name="attributeQuerySoapUsername">test_ping</s:key>
      <s:key name="attributeQueryTTL">3600</s:key>
      <s:key name="attribute_aliases"/>
      <s:key name="blacklistedAutoMappedRoles">
        <s:list/>
      </s:key>
      <s:key name="blacklistedUsers">
        <s:list/>
      </s:key>
      <s:key name="caCertFile">/opt/splunk/etc/auth/cacert.pem</s:key>
      <s:key name="cipherSuite"></s:key>
      <s:key name="defaultRoleIfMissing"></s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="ecdhCurves"></s:key>
      <s:key name="entityId">someOtherEntityId</s:key>
      <s:key name="errorUrl"></s:key>
      <s:key name="errorUrlLabel"></s:key>
      <s:key name="fqdn">http://so1</s:key>
      <s:key name="idpCertChains">
        <s:list/>
      </s:key>
      <s:key name="idpCertPath"></s:key>
      <s:key name="maxAttributeQueryQueueSize">100</s:key>
      <s:key name="maxAttributeQueryThreads">2</s:key>
      <s:key name="nameIdFormat"></s:key>
      <s:key name="protocol_endpoints">
        <s:dict>
          <s:key name="idpAttributeQueryUrl">https://saml-idp:9999/idp/attrsvc.ssaml2</s:key>
          <s:key name="idpSLOUrl"></s:key>
          <s:key name="idpSSOUrl">https://saml-idp:9999/idp/SSO.saml2</s:key>
          <s:key name="issuerId"></s:key>
        </s:dict>
      </s:key>
      <s:key name="redirectAfterLogoutToUrl">http://www.splunk.com</s:key>
      <s:key name="redirectPort">12800</s:key>
      <s:key name="replicateCertificates">1</s:key>
      <s:key name="signAuthnRequest">1</s:key>
      <s:key name="signatureAlgorithm">
        <s:dict>
          <s:key name="name">RSA-SHA1</s:key>
          <s:key name="uri">http://www.w3.org/2000/09/xmldsig#rsa-sha1</s:key>
        </s:dict>
      </s:key>
      <s:key name="signedAssertion">1</s:key>
      <s:key name="singleLogoutServiceUrl">http://so1:12800/saml/logout</s:key>
      <s:key name="skipAttributeQueryRequestForUsers">
        <s:list/>
      </s:key>
      <s:key name="sloBinding">HTTPPost</s:key>
      <s:key name="spCertPath">/opt/splunk/etc/auth/server.pem</s:key>
      <s:key name="sslAltNameToCheck"></s:key>
      <s:key name="sslCommonNameToCheck"></s:key>
      <s:key name="sslKeysfile">/opt/splunk/etc/auth/server.pem</s:key>
      <s:key name="sslKeysfilePassword">******</s:key>
      <s:key name="sslVerifyServerCert">false</s:key>
      <s:key name="sslVersions">SSL3,TLS1.0,TLS1.1,TLS1.2</s:key>
      <s:key name="ssoBinding">HTTPPost</s:key>
      <s:key name="uiStatusPage">/account/status</s:key>
    </s:dict>
  </content>
</entry>
```

authentication/providers/SAML/{stanza_name}/enable

```
https://<host>:<mPort>/services/authentication/providers/SAML/{stanza_name}/enable
```

POST

Enable a SAML strategy.

Request parameters
None

Returned values
None

Example request

```
curl -k -u admin:password -X POST
https://localhost:8089/services/authentication/providers/SAML/my_strategy/enable
```

authentication/providers/SAML/{stanza_name}/disable

```
https://<host>:<mPort>/services/authentication/providers/SAML/{stanza_name}/disable
```

POST

Delete a SAML strategy.

Request parameters
None

Returned values
None

Example request

```
curl -k -u admin:password -X POST
https://localhost:8089/services/authentication/providers/SAML/my_strategy/disable
```

auth/login

```
https://<host>:<mPort>/services/auth/login
```

Get a session ID for use in subsequent API calls that require authentication. Set up cookie-based authorization.

The splunkd server supports token-based authentication using the standard HTTP authorization header. Before you can access Splunk Enterprise resources, you must authenticate with the splunkd server using your username and password.

Use cookie-based authorization

To use cookie-based authorization, first ensure that the `allowCookieAuth` setting is enabled in `server.conf`. By default, this setting is enabled in Splunk software versions 6.2 and later.

If `allowCookieAuth` is enabled, you can pass a `cookie=1` parameter to the POST request on `auth/login`. As noted in the *Response data keys* section below, a `Set-Cookie` header is returned. This header must be used in subsequent requests.

Any request authenticated using a cookie may include a new `Set-Cookie` header in its response. Use this new cookie value in any subsequent requests.

If you do not receive a `Set-Cookie` header in response to the auth/login POST request but login succeeded, you can use the standard `Authorization:Splunk...` header with the session key for authorization.

See also

- Authentication
- authentication/current-context

POST

Get a session ID for use in subsequent API calls that require authentication. Optionally, use cookie-based authentication or multifactor authentication.

Request parameters

Name	Type	Description
cookie	Boolean, only used value is 1.	To use cookie-based REST auth, pass in `cookie=1`. Cookies will only be returned if the cookie parameter is passed in with the value of 1.
password	String	**Required**. Current *username* password.
passcode	String	**Required for users with RSA multifactor authentication**. The passcode associated with RSA multifactor authentication. This is a combination of the user's RSA token and PIN.
username	String	**Required**. Authenticated session owner name.

Response data keys

> **Note:** Only a `<response>` element is returned instead of a full `<atom>` feed.

Name	Description
sessionKey	Session ID.

A `Set-Cookie` HTTP header is returned if cookie-based authentication is requested.

Failure to authenticate returns the following response.

```
<response>
     <messages>
         <msg type="WARN">Login failed</msg>
     </messages>
</response>
```

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/auth/login -d username=admin -d
password=changeme
```

XML Response

```
<response>
    <sessionKey>192fd3e46a31246da7ea7f109e7f95fd</sessionKey>
</response>
```

Example request and response using RSA passcode

XML Request

```
curl -k https://tsen-centos62x64-7:8089/services/auth/login -d username=john@test-splunk.com -d
password=changed123 -d passcode='gq!k##9b'
```

XML Response

```
<response>
<sessionKey>8Q1QczpArNgKqfUmkmhwgiZVEr4^phZzEbX9NGonO^EdW8DOKXHR9iXNStzAEpVteSkShTxS^8QcyZ8zYj4P812iRBskRurK
_RZ2dEy7FZjYoaLG0wx2rkSS0sIc</sessionKey>
</response>
<messages>
    <msg code=""></msg>
  </messages>
  </response>
```

Example failed login with missing RSA passcode

XML Request

```
curl -k https://tsen-centos62x64-7:8089/services/auth/login -d username=john@test-splunk.com -d
password='changed123:gq!k##9b'
```

XML Response

```
<response>
  <messages>
    <msg type="WARN" code="incorrect_username_or_password">Login failed</msg>
  </messages>
</response>
```

authentication/current-context

```
https://<host>:<mPort>/services/authentication/current-context
```

Get the authenticated session owner username.

For additional information, see the following resources.

- auth/login
- List of available capabilities in *Securing Splunk Enterprise*.

GET

Get user information for the current context.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
capabilities	List of capabilities assigned to role.
defaultApp	Default app for the user, which is invoked at login.
defaultAppIsUserOverride	Default app override indicates: `true` = Default app overrides the user role default app. `false` = Default app does not override the user role default app.
defaultAppSourceRole	The role that determines the default app for the user, if the user has multiple roles.
email	User email address.
password	User password.
realname	User full name.
restart_background_jobs	Restart background search job that has not completed when Splunk restarts indication: `true` = Restart job. `false` = Do not restart job.
roles	Roles assigned to the user.
type	User authentication system type: • `LDAP` • `Scripted` • `Splunk` • `System` (reserved for system user)
tz	User timezone.
username	Authenticated session owner name.

Usage in search

Here is an example of calling this endpoint in a search command to get the current user.

```
... rest /services/authentication/current-context/context | fields + username ...
```

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/current-context
```

XML Response

```
.
.
.
<title>current-context</title>
 <id>https://localhost:8089/services/authentication/current-context</id>
 <updated>2014-06-30T11:26:19-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>context</title>
   <id>https://localhost:8089/services/authentication/current-context/context</id>
   <updated>2014-06-30T11:26:19-07:00</updated>
   <link href="/services/authentication/current-context/context" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/current-context/context" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list>
           <s:item>accelerate_datamodel</s:item>
           <s:item>accelerate_search</s:item>
           <s:item>admin_all_objects</s:item>
           <s:item>change_authentication</s:item>
           <s:item>change_own_password</s:item>
           <s:item>edit_deployment_client</s:item>
           <s:item>edit_deployment_server</s:item>
           <s:item>edit_dist_peer</s:item>
           <s:item>edit_forwarders</s:item>
           <s:item>edit_httpauths</s:item>
           <s:item>edit_input_defaults</s:item>
           <s:item>edit_monitor</s:item>
           <s:item>edit_roles</s:item>
           <s:item>edit_scripted</s:item>
           <s:item>edit_search_server</s:item>
           <s:item>edit_server</s:item>
           <s:item>edit_splunktcp</s:item>
           <s:item>edit_splunktcp_ssl</s:item>
           <s:item>edit_tcp</s:item>
           <s:item>edit_udp</s:item>
           <s:item>edit_user</s:item>
           <s:item>edit_view_html</s:item>
           <s:item>edit_web_settings</s:item>
           <s:item>edit_win_admon</s:item>
           <s:item>edit_win_eventlogs</s:item>
           <s:item>edit_win_perfmon</s:item>
           <s:item>edit_win_regmon</s:item>
           <s:item>edit_win_wmiconf</s:item>
           <s:item>embed_report</s:item>
           <s:item>get_diag</s:item>
           <s:item>get_metadata</s:item>
           <s:item>get_typeahead</s:item>
           <s:item>indexes_edit</s:item>
           <s:item>input_file</s:item>
```

```
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">1</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">system</s:key>
  </s:dict>
</s:key>
<s:key name="email">changeme@example.com</s:key>
<s:key name="password">********</s:key>
<s:key name="realname">Administrator</s:key>
<s:key name="restart_background_jobs">1</s:key>
<s:key name="roles">
  <s:list>
    <s:item>admin</s:item>
  </s:list>
</s:key>
<s:key name="type">Splunk</s:key>
```

```
      <s:key name="tz"></s:key>
      <s:key name="username">admin</s:key>
    </s:dict>
  </content>
</entry>
```

authentication/httpauth-tokens

`https://<host>:<mPort>/services/authentication/httpauth-tokens`

List currently active session IDs and users.

For additional information, see the following resources.

- auth/login
- authentication/current-context

GET

List currently active session IDs/users.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
authString	Unique identifier for this session.
searchId	Search ID associated with the session, if it was created for a search job. If it is a login-type session, the value is empty. The session ID token is valid for the duration of the web session.
timeAccessed	Last time the session was touched.
userName	Username associated with the session.

Usage in searches

Here is an example of calling this endpoint in a search.

```
| rest /services/authentication/httpauth-tokens | search (NOT userName="splunk-system-user") searchId="" |
table userName splunk_server timeAccessed
```

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/httpauth-tokens
```

XML Response

```
.
.
.
<title>httpauth-tokens</title>
 <id>https://localhost:8089/services/authentication/httpauth-tokens</id>
 <updated>2014-06-30T11:28:04-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>2</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>15a773187d3e4437cbe9809f41f23d8f</title>
   <id>https://localhost:8089/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f</id>
   <updated>2014-06-30T11:28:04-07:00</updated>
   <link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="list"/>
   <link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="authString">vdZv2eB9F0842dyJhrIEiGNTcBMpBeGuwGPYxtGLKAESQkzjSjG7dbymQW58y^oI3kxYXWfK
_Fd3cRGqwPQGp58RvEkzwCaC6PmQgCsK</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="searchId"></s:key>
       <s:key name="timeAccessed">Mon Jun 30 11:28:04 2014</s:key>
       <s:key name="userName">admin</s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>694ef5bda40ae8c4f59626671b5f0c9a</title>
   <id>https://localhost:8089/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a</id>
   <updated>2014-06-30T11:28:04-07:00</updated>
   <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="list"/>
   <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="authString">1RU5vGFm2OPq29plLtvqlEB9xzPDLZ3AleUhE1bwPjIrKtvyLE4fODhs^TgI4
_NamvVtqusj8GnnNxd5wBB1wT^qHXn1DOV7LcCvErpyTzOvISr^2TnKUC</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="searchId"></s:key>
       <s:key name="timeAccessed">Mon Jun 30 11:26:09 2014</s:key>
       <s:key name="userName">splunk-system-user</s:key>
     </s:dict>
   </content>
 </entry>
```

authentication/httpauth-tokens/{name}

```
https://<host>:<mPort>/services/authentication/httpauth-tokens/<name>
```

Access or delete the `{name}` session, where `{name}` is the session ID returned by auth/login.

For additional information, see the following resources.

- auth/login
- authentication/current-context

DELETE

Delete the session associated with this session ID.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/authentication/httpauth-tokens
/vdZv2eB9F0842dyJhrIEiGNTcBMpBeGuwGPYxtGLKAESQkzjSjG7dbymQW58y^oI3kxYXWfK_Fd3cRGqwPQGp58RvEkzwCaC6PmQgCsK
```

XML Response

```
.
.
.
<title>httpauth-tokens</title>
 <id>https://localhost:8089/services/authentication/httpauth-tokens</id>
 <updated>2014-06-30T12:02:12-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>694ef5bda40ae8c4f59626671b5f0c9a</title>
   <id>https://localhost:8089/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a</id>
   <updated>2014-06-30T12:02:12-07:00</updated>
   <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="list"/>
   <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="authString">1RU5vGFm2OPq29plLtvqlEB9xzPDLZ3AleUhE1bwPjIrKtvyLE4fODhs^TgI4
_NamvVtqusj8GnnNxd5wBB1wT^qHXn1DOV7LcCvErpyTzOvISr^2TnKUC</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
```

```
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="searchId"></s:key>
       <s:key name="timeAccessed">Mon Jun 30 11:42:31 2014</s:key>
       <s:key name="userName">splunk-system-user</s:key>
     </s:dict>
   </content>
 </entry>
```

GET

Get session information.

Request parameters

None

Response keys

Name	Description
authString	Unique session identifier.
searchId	Session search ID, if it is a search job session. The value is blank for a login-type session.
timeAccessed	Last time the session was touched.
userName	Username associated with the session.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/httpauth-tokens
/vdZv2eB9F0842dyJhrIEiGNTcBMpBeGuwGPYxtGLKAESQkzjSjG7dbymQW58y^oI3kxYXWfK_Fd3cRGqwPQGp58RvEkzwCaC6PmQgCsK
```

XML Response

```
.
.
.
```

```
 <title>httpauth-tokens</title>
 <id>https://localhost:8089/services/authentication/httpauth-tokens</id>
 <updated>2014-06-30T11:39:52-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>15a773187d3e4437cbe9809f41f23d8f</title>
   <id>https://localhost:8089/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f</id>
   <updated>2014-06-30T11:39:52-07:00</updated>
   <link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="list"/>
   <link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="authString">vdZv2eB9F0842dyJhrIEiGNTcBMpBeGuwGPYxtGLKAESQkzjSjG7dbymQW58y^oI3kxYXWfK
_Fd3cRGqwPQGp58RvEkzwCaC6PmQgCsK</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list/>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
```

```
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="searchId"></s:key>
      <s:key name="timeAccessed">Mon Jun 30 11:39:52 2014</s:key>
      <s:key name="userName">admin</s:key>
    </s:dict>
  </content>
</entry>
```

authentication/users

`https://<host>:<mPort>/services/authentication/users`

List current users and create new users.

For additional information about configuring users and roles, see the following resources in *Securing Splunk Enterprise*.

- About configuring role-based user access
- Securing Splunk Enterprise
- List of available capabilities

Authentication and authorization
Requires the `edit_user` capability.

GET

List current users.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
capabilities	List of capabilities assigned to role.
defaultApp	Default app for the user, which is invoked at login.
defaultAppIsUserOverride	Default app override indicates: `true` = Default app overrides the user role default app. `false` = Default app does not override the user role default app.
defaultAppSourceRole	The role that determines the default app for the user, if the user has multiple roles.
email	User email address.
locked-out	Returns `1` if the user is locked out, and `0` if the user is not locked out.
password	User password.
realname	User full name.

Name	Description
restart_background_jobs	Restart background search job that has not completed when Splunk restarts indication: `true` = Restart job. `false` = Do not restart job.
roles	Roles assigned to the user.
type	One of the following user authentication system types. • `LDAP` • `Scripted` • `Splunk` • `System` (reserved for system user)
tz	User timezone.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/users
```

XML Response

```
.
.
.
 <title>users</title>
 <id>https://localhost:8089/services/authentication/users</id>
 <updated>2014-06-30T12:27:48-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authentication/users/_new" rel="create"/>
 <opensearch:totalResults>2</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>admin</title>
   <id>https://localhost:8089/services/authentication/users/admin</id>
   <updated>2014-06-30T12:27:48-07:00</updated>
   <link href="/services/authentication/users/admin" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/users/admin" rel="list"/>
   <link href="/services/authentication/users/admin" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list>
           <s:item>accelerate_datamodel</s:item>
           <s:item>accelerate_search</s:item>
           <s:item>admin_all_objects</s:item>
           <s:item>change_authentication</s:item>
           <s:item>change_own_password</s:item>
           <s:item>edit_deployment_client</s:item>
```

```
    <s:item>edit_deployment_server</s:item>
    <s:item>edit_dist_peer</s:item>
    <s:item>edit_forwarders</s:item>
    <s:item>edit_httpauths</s:item>
    <s:item>edit_input_defaults</s:item>
    <s:item>edit_monitor</s:item>
    <s:item>edit_roles</s:item>
    <s:item>edit_scripted</s:item>
    <s:item>edit_search_server</s:item>
    <s:item>edit_server</s:item>
    <s:item>edit_splunktcp</s:item>
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">1</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
```

```
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="email">changeme@example.com</s:key>
      <s:key name="password">********</s:key>
      <s:key name="realname">Administrator</s:key>
      <s:key name="restart_background_jobs">1</s:key>
      <s:key name="roles">
        <s:list>
          <s:item>admin</s:item>
        </s:list>
      </s:key>
      <s:key name="type">Splunk</s:key>
      <s:key name="tz"></s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>user1</title>
  <id>https://localhost:8089/services/authentication/users/user1</id>
  <updated>2014-06-30T12:27:48-07:00</updated>
  <link href="/services/authentication/users/user1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/user1" rel="list"/>
  <link href="/services/authentication/users/user1" rel="edit"/>
  <link href="/services/authentication/users/user1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
    <s:item>edit_server</s:item>
    <s:item>edit_splunktcp</s:item>
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">0</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
```

```
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="email"></s:key>
       <s:key name="password">********</s:key>
       <s:key name="realname"></s:key>
       <s:key name="restart_background_jobs">1</s:key>
       <s:key name="roles">
         <s:list>
           <s:item>admin</s:item>
         </s:list>
       </s:key>
       <s:key name="type">Splunk</s:key>
       <s:key name="tz"></s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Create a user.

Usage details

When creating a user you must specify at least one role.

Specify one or more roles for the user. You can create a new role for the user by setting the `createrole` parameter to "true" and specify the new role name as a `roles` parameter value.

Request parameters

Name	Datatype	Description
createrole	Boolean	Flag to indicate that a new role should be created for the user. If set to "true", the new role `user-<name>` is created and assigned to the user. The `<name>` portion of the new role matches the `name` parameter value passed in with this POST request. If set to "false", at least one existing role must be specified using the `roles` parameter for the POST request. Defaults to "false".
defaultApp	String	User default app. Overrides the default app inherited from the user roles.
email	String	User email address.
force-change-pass	Boolean	Force user to change password indication: `true` = Force password change. `false` = Do not force password change.
name	String	**Required**. Unique user login name.
password	String	User login password.
realname	String	Full user name.

Name	Datatype	Description
restart_background_jobs	Boolean	Restart background search job that has not completed when Splunk restarts indication: `true` = Restart job. `false` = Do not restart job.
roles	String	Role to assign to this user. To assign multiple roles, pass in each role using a separate `roles` parameter value. For example, `-d roles="role1", -d roles="role2"`. At least one existing role is required if you are not using the `createrole` parameter to create a new role for the user. If you are using `createrole` to create a new role, you can optionally use this parameter to specify additional roles to assign to the user.
tz	String	User timezone.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/users -d name=User1 -d
password=changeme -d roles=admin
```

XML Response

```
<title>users</title>
 <id>https://localhost:8089/services/authentication/users</id>
 <updated>2014-06-30T12:18:19-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authentication/users/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>user1</title>
   <id>https://localhost:8089/services/authentication/users/user1</id>
   <updated>2014-06-30T12:18:19-07:00</updated>
   <link href="/services/authentication/users/user1" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/users/user1" rel="list"/>
   <link href="/services/authentication/users/user1" rel="edit"/>
   <link href="/services/authentication/users/user1" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list>
           <s:item>accelerate_datamodel</s:item>
           <s:item>accelerate_search</s:item>
           <s:item>admin_all_objects</s:item>
           <s:item>change_authentication</s:item>
           <s:item>change_own_password</s:item>
```

```
    <s:item>edit_deployment_client</s:item>
    <s:item>edit_deployment_server</s:item>
    <s:item>edit_dist_peer</s:item>
    <s:item>edit_forwarders</s:item>
    <s:item>edit_httpauths</s:item>
    <s:item>edit_input_defaults</s:item>
    <s:item>edit_monitor</s:item>
    <s:item>edit_roles</s:item>
    <s:item>edit_scripted</s:item>
    <s:item>edit_search_server</s:item>
    <s:item>edit_server</s:item>
    <s:item>edit_splunktcp</s:item>
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">0</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
```

```
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="email"></s:key>
      <s:key name="password">********</s:key>
      <s:key name="realname"></s:key>
      <s:key name="restart_background_jobs">1</s:key>
      <s:key name="roles">
        <s:list>
          <s:item>admin</s:item>
        </s:list>
      </s:key>
      <s:key name="type">Splunk</s:key>
      <s:key name="tz"></s:key>
    </s:dict>
  </content>
</entry>
```

authentication/users/{name}

`https://<host>:<mPort>/services/authentication/users/{name}`

Access and update user information or delete the `{name}`> user.

Usage details

The `/{name}` username portion of the URL is not case sensitive.

For additional information about user capabiilties, see the following resource in *Securing Splunk Enterprise*.

- List of available capabilities

Authentication and authorization

Requires the `edit_user` capability.

DELETE

Remove the specified user from the system.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/authentication/users/user1
```

XML Response

```
.
.
.
 <title>users</title>
 <id>https://localhost:8089/services/authentication/users</id>
 <updated>2014-06-30T12:51:09-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authentication/users/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>admin</title>
   <id>https://localhost:8089/services/authentication/users/admin</id>
   <updated>2014-06-30T12:51:09-07:00</updated>
   <link href="/services/authentication/users/admin" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/users/admin" rel="list"/>
   <link href="/services/authentication/users/admin" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list>
           <s:item>accelerate_datamodel</s:item>
           <s:item>accelerate_search</s:item>
           <s:item>admin_all_objects</s:item>
           <s:item>change_authentication</s:item>
           <s:item>change_own_password</s:item>
           <s:item>edit_deployment_client</s:item>
           <s:item>edit_deployment_server</s:item>
           <s:item>edit_dist_peer</s:item>
           <s:item>edit_forwarders</s:item>
           <s:item>edit_httpauths</s:item>
           <s:item>edit_input_defaults</s:item>
           <s:item>edit_monitor</s:item>
           <s:item>edit_roles</s:item>
```

```
    <s:item>edit_scripted</s:item>
    <s:item>edit_search_server</s:item>
    <s:item>edit_server</s:item>
    <s:item>edit_splunktcp</s:item>
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">1</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>admin</s:item>
            <s:item>splunk-system-role</s:item>
          </s:list>
```

```
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="email">changeme@example.com</s:key>
      <s:key name="password">********</s:key>
      <s:key name="realname">Administrator</s:key>
      <s:key name="restart_background_jobs">1</s:key>
      <s:key name="roles">
        <s:list>
          <s:item>admin</s:item>
        </s:list>
      </s:key>
      <s:key name="type">Splunk</s:key>
      <s:key name="tz"></s:key>
    </s:dict>
  </content>
</entry>
```

GET

Return information for the specified user.

Request parameters

None

Response keys

Name	Description
capabilities	List of capabilities assigned to role.
defaultApp	Default app for the user, which is invoked at login.
defaultAppIsUserOverride	Default app override indicator. `true` = Default app overrides the user role default app. `false` = Default app does not override the user role default app.
defaultAppSourceRole	Role that determines the default app for the user, if the user has multiple roles.
email	User email address
locked-out	Returns `1` if the user is locked out, and `0` if the user is not locked out.
password	User password
realname	User full name
restart_background_jobs	Indicates whether incomplete background search jobs restart when the Splunk deployment restarts. `true` = Restart jobs.

Name	Description
	`false` = Do not restart jobs.
roles	Roles assigned to the user.
type	One of the following user authentication system types. • `LDAP` • `Scripted` • `Splunk` • `System` (reserved for system user)
tz	User timezone.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/users/user1
```

XML Response

```
.
.
.
<title>users</title>
 <id>https://localhost:8089/services/authentication/users</id>
 <updated>2014-06-30T12:39:18-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authentication/users/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>user1</title>
   <id>https://localhost:8089/services/authentication/users/user1</id>
   <updated>2014-06-30T12:39:18-07:00</updated>
   <link href="/services/authentication/users/user1" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/users/user1" rel="list"/>
   <link href="/services/authentication/users/user1" rel="edit"/>
   <link href="/services/authentication/users/user1" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list>
           <s:item>accelerate_datamodel</s:item>
           <s:item>accelerate_search</s:item>
           <s:item>admin_all_objects</s:item>
           <s:item>change_authentication</s:item>
           <s:item>change_own_password</s:item>
           <s:item>edit_deployment_client</s:item>
           <s:item>edit_deployment_server</s:item>
```

```
    <s:item>edit_dist_peer</s:item>
    <s:item>edit_forwarders</s:item>
    <s:item>edit_httpauths</s:item>
    <s:item>edit_input_defaults</s:item>
    <s:item>edit_monitor</s:item>
    <s:item>edit_roles</s:item>
    <s:item>edit_scripted</s:item>
    <s:item>edit_search_server</s:item>
    <s:item>edit_server</s:item>
    <s:item>edit_splunktcp</s:item>
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">0</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
```

```
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list>
               <s:item>defaultApp</s:item>
               <s:item>email</s:item>
               <s:item>force-change-pass</s:item>
               <s:item>password</s:item>
               <s:item>realname</s:item>
               <s:item>restart_background_jobs</s:item>
               <s:item>roles</s:item>
               <s:item>tz</s:item>
             </s:list>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="email"></s:key>
       <s:key name="password">********</s:key>
       <s:key name="realname"></s:key>
       <s:key name="restart_background_jobs">1</s:key>
       <s:key name="roles">
         <s:list>
           <s:item>admin</s:item>
         </s:list>
       </s:key>
       <s:key name="type">Splunk</s:key>
       <s:key name="tz"></s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Update the specified user.

Request parameters

Name	Type	Description

defaultApp	String	User default app. This overrides the default app inherited from the user roles.
email	String	User email address.
force-change-pass	Boolean	Indicates whether to force user password change. `true` = Force password change. `false` = Do not force password change.
oldpassword	String	Old user login password. Only **required** if using the *password* parameter to change the current user's password.
password	String	**Required**. User login password. To change the user password, enter the new user login password here. To change the current user's password, also supply the old password in the *oldpassword* parameter.
realname	String	Full user name.
restart_background_jobs	Boolean	Indicates whether to restart background search job that has not completed when the Splunk deployment restarts. `true` = Restart job. `false` = Do not restart job.
roles	String	Role to assign to this user. To assign multiple roles, pass in each role using a separate `roles` parameter value. For example, `-d roles="role1", -d roles="role2"`. At least one existing role is required if you are not using the `createrole` parameter to create a new role for the user. If you are using `createrole` to create a new role, you can optionally use this parameter to specify additional roles to assign to the user.
tz	String	User timezone.

Response keys

Name	Description
capabilities	List of capabilities assigned to role.
defaultApp	Default app for the user, which is invoked at login.
defaultAppIsUserOverride	Default app override indicator. `true` = Default app overrides the user role default app. `false` = Default app does not override the user role default app.
defaultAppSourceRole	Role that determines the default app for the user, if the user has multiple roles.
email	User email address.
password	User password.
realname	User full name.
restart_background_jobs	Indicates whether to restart background search job that has not completed when the Splunk deployment restarts. `true` = Restart job. `false` = Do not restart job.
roles	Roles assigned to the user.
type	One of the following user authentication system types. • `LDAP` • `Scripted` • `Splunk` • `System` (reserved for system user)
tz	User timezone.

Name	Description

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/users/user1 -d defaultApp=launcher
```

XML Response

```
.
.
.
<title>users</title>
 <id>https://localhost:8089/services/authentication/users</id>
 <updated>2014-06-30T12:45:23-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authentication/users/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>user1</title>
   <id>https://localhost:8089/services/authentication/users/user1</id>
   <updated>2014-06-30T12:45:23-07:00</updated>
   <link href="/services/authentication/users/user1" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authentication/users/user1" rel="list"/>
   <link href="/services/authentication/users/user1" rel="edit"/>
   <link href="/services/authentication/users/user1" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list>
           <s:item>accelerate_datamodel</s:item>
           <s:item>accelerate_search</s:item>
           <s:item>admin_all_objects</s:item>
           <s:item>change_authentication</s:item>
           <s:item>change_own_password</s:item>
           <s:item>edit_deployment_client</s:item>
           <s:item>edit_deployment_server</s:item>
           <s:item>edit_dist_peer</s:item>
           <s:item>edit_forwarders</s:item>
           <s:item>edit_httpauths</s:item>
           <s:item>edit_input_defaults</s:item>
           <s:item>edit_monitor</s:item>
           <s:item>edit_roles</s:item>
           <s:item>edit_scripted</s:item>
           <s:item>edit_search_server</s:item>
           <s:item>edit_server</s:item>
           <s:item>edit_splunktcp</s:item>
```

```
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">1</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>*</s:item>
          </s:list>
```

```
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="email"></s:key>
       <s:key name="password">********</s:key>
       <s:key name="realname"></s:key>
       <s:key name="restart_background_jobs">1</s:key>
       <s:key name="roles">
         <s:list>
           <s:item>admin</s:item>
         </s:list>
       </s:key>
       <s:key name="type">Splunk</s:key>
       <s:key name="tz"></s:key>
     </s:dict>
   </content>
 </entry>
```

authorization/capabilities

`https://<host>:<mPort>/services/authorization/capabilities`

Access system capabilities.

GET

List system capabiilities.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
capabilities	List of capabilities assigned to role.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/capabilities
```

XML Response

```
.
.
.
<title>capabilities</title>
 <id>https://localhost:8089/services/authorization/capabilities</id>
 <updated>2014-06-30T12:56:35-07:00</updated>
```

```
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>capabilities</title>
  <id>https://localhost:8089/services/authorization/capabilities/capabilities</id>
  <updated>2014-06-30T12:56:35-07:00</updated>
  <link href="/services/authorization/capabilities/capabilities" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/capabilities/capabilities" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>delete_by_keyword</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>edit_splunktcp</s:item>
          <s:item>edit_splunktcp_ssl</s:item>
          <s:item>edit_tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
          <s:item>edit_web_settings</s:item>
          <s:item>edit_win_admon</s:item>
          <s:item>edit_win_eventlogs</s:item>
          <s:item>edit_win_perfmon</s:item>
          <s:item>edit_win_regmon</s:item>
          <s:item>edit_win_wmiconf</s:item>
          <s:item>embed_report</s:item>
          <s:item>get_diag</s:item>
          <s:item>get_metadata</s:item>
          <s:item>get_typeahead</s:item>
          <s:item>indexes_edit</s:item>
          <s:item>input_file</s:item>
          <s:item>license_edit</s:item>
          <s:item>license_tab</s:item>
          <s:item>list_deployment_client</s:item>
          <s:item>list_deployment_server</s:item>
          <s:item>list_forwarders</s:item>
          <s:item>list_httpauths</s:item>
          <s:item>list_inputs</s:item>
          <s:item>list_pdfserver</s:item>
          <s:item>list_win_localavailablelogs</s:item>
          <s:item>output_file</s:item>
          <s:item>request_remote_tok</s:item>
          <s:item>rest_apps_management</s:item>
          <s:item>rest_apps_view</s:item>
          <s:item>rest_properties_get</s:item>
          <s:item>rest_properties_set</s:item>
          <s:item>restart_splunkd</s:item>
          <s:item>rtsearch</s:item>
          <s:item>run_debug_commands</s:item>
          <s:item>schedule_rtsearch</s:item>
          <s:item>schedule_search</s:item>
          <s:item>search</s:item>
          <s:item>use_file_operator</s:item>
          <s:item>write_pdfserver</s:item>
        </s:list>
      </s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

authorization/fieldfilters

`https://<host>:<mPort>/services/authorization/fieldfilters`

Create a field filter or get a list of field filters. See Protect PII, PHI, and other sensitive data with field filters in *Securing Splunk Platform*.

READ THIS FIRST: Should you deploy field filters in your organization?

Field filters are a powerful tool that can help many organizations protect their sensitive fields from prying eyes, but it might not be a good fit for everyone. If your organization runs Splunk Enterprise Security or if your users rely heavily on commands that field filters restricts by default (`mpreview`, `mstats`, `tstats`, `typeahead`, and `walklex`), do not use field filters in production until you have thoroughly planned how you will work around these restricted commands. See READ THIS: Restricted commands do not work in searches on indexes that have field filters in *Securing Splunk platform*.

GET

List all field filters. To use GET with this endpoint, you must be a member of the admin, sc_admin, or power user role.

Request parameters

None

Response keys

Name	Description
"name": "A field filter name"	The name of the field filter. Field filter names can contain only alphanumeric characters and underscores (_). Spaces and special symbols are not allowed.
action.field	The name of the field to filter for this action.
action.operator	The operator for the action. Operators for actions are described as follows: • null(): Removes the field value from results of searches to which this filter is applied. • sha256(): Computes and returns the secure hash of the value of the field based on the FIPS-compliant SHA-256 (SHA-2 family) hash function. This hash is then used to replace the value of the field wherever it appears in results of searches to which this filter is applied. See Cryptographic functions in the Splunk Cloud Platform *Search Reference*. • sha512(): Computes and returns the secure hash of the value of the field based on the FIPS-compliant SHA-512 (SHA-2 family) hash function. This hash is then used to replace the value of the field wherever it appears in results of searches to which this filter is applied. See Cryptographic functions in the Splunk Cloud Platform *Search Reference*. • <string literal>: Replaces the fieldname value with the specified string wherever the field value appears in results of searches to which this filter is applied. A string literal is a sequence of characters enclosed in double quotation marks (" "). Use backslash (\ ) to escape the \ and " characters in a string literal. For example, use \\ and \" . • sed(<string literal>): For _raw fields. The sed expression acts on searches to which this filter is applied. The sed expression replaces strings in search results that are matched by a regular expression `(s)` or transliterates characters found in search results with corresponding characters provided by the sed expression `(y)`. A string literal is a sequence of characters enclosed in double quotation marks (" "). Use backslash (\ ) to escape the \ and " characters in a string literal. For example, use \\ and \" .
"description": "A field filter description"	Stores a description of the field filter.
"index": "One or more index names"	Specifies an index name or a list of comma-separated index names of the target indexes you want to search that contain the data you want to protect. If an index is not specified, all indexes are searched.
limit.key	The key for the field filter limit, which limits the field filter to events with a specific target host, source, or sourcetype. You can specify only one value. If the limit key is empty, the field filter doesn't apply to events with a specific host, source, or sourcetype. Limit statements that include wildcards or the following operators are not supported: AND, OR.
limit.value	The value for the limit, which is a sequence of characters enclosed in double quotation marks (") that represents the name of the hosts, the sources, or the source types. The limit value can be a value or a list of comma-separated values for the specified limit.
"roleExemptions": [	A list of field filters from which each role is exempt. If a role is exempt from a field filter, the field filter is not run at search time for any users holding this role. Roles inherit all field filter exemptions from imported roles. You can't remove

Name	Description
list of exempted roles]	inherited field filter exemptions.

Example request and response

XML Request

```
$ curl -sk -u admin:changeme https://localhost:8106/services/authorization/fieldfilters
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>fieldfilters</title>
  <id>https://localhost:8106/services/authorization/fieldfilters</id>
  <updated>2023-09-07T20:54:51+00:00</updated>
  <generator build="4464e07e99dad5532f25c08d83b3af6675536bdf" version="20230907"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/fieldfilters/_new" rel="create"/>
  <link href="/services/authorization/fieldfilters/_reload" rel="_reload"/>
  <link href="/services/authorization/fieldfilters/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>demofilter</title>
    <id>https://localhost:8106/servicesNS/nobody/search/authorization/fieldfilters/demofilter</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demofilter" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demofilter" rel="list"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demofilter/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demofilter" rel="edit"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demofilter" rel="remove"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demofilter/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action">
          <s:dict>
            <s:key name="field">bytes</s:key>
            <s:key name="operator">"HIDDEN"</s:key>
          </s:dict>
        </s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="limit"/>
        <s:key name="roleExemptions">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a field filter. To use POST with this endpoint, you must be a member of the admin or sc_admin role.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8106/servicesNS/nobody/system/authorization/fieldfilters/ -d
name=demo_hash_filter -d action=\"fieldName\"=sha256\(\)
```

XML Response

If a filter filter with the specified name already exists, an error is returned. If the field filter is successfully created, the newly created field filter is returned.

The following is the XML response:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>fieldfilters</title>
  <id>https://localhost:8106/servicesNS/nobody/system/authorization/fieldfilters</id>
  <updated>2023-09-07T22:11:14+00:00</updated>
  <generator build="4464e07e99dad5532f25c08d83b3af6675536bdf" version="20230907"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/system/authorization/fieldfilters/_new" rel="create"/>
  <link href="/servicesNS/nobody/system/authorization/fieldfilters/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/authorization/fieldfilters/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>demo_hash_filter</title>
    <id>https://localhost:8106/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="list"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="edit"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="remove"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action">
          <s:dict>
            <s:key name="field">fieldName</s:key>
            <s:key name="operator">sha256()</s:key>
          </s:dict>
        </s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="limit"/>
        <s:key name="roleExemptions">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

authorization/fieldfilters/{name}

`https://<host>:<mPort>/services/authorization/fieldfilters/<name>`

Access, create, or delete properties for the {name} field filter. See Protect PII, PHI, and other sensitive data with field filters in *Securing Splunk Platform*.

READ THIS FIRST: Should you deploy field filters in your organization?
Field filters are a powerful tool that can help many organizations protect their sensitive fields from prying eyes, but it might not be a good fit for everyone. If your organization runs Splunk Enterprise Security or if your users rely heavily on commands that field filters restricts by default (`mpreview`, `mstats`, `tstats`, `typeahead`, and `walklex`), do not use field filters in production until you have thoroughly planned how you will work around these restricted commands. See READ THIS: Restricted commands do not work in searches on indexes that have field filters in *Securing Splunk platform*.

DELETE

Delete the specified field filter. To use DELETE with this endpoint, you must be a member of the admin or sc_admin role.

Request parameters
None

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE
https://localhost:8106/services/authorization/fieldfilters/demo_hash_filter
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>fieldfilters</title>
  <id>https://localhost:8106/services/authorization/fieldfilters</id>
  <updated>2023-09-07T22:22:48+00:00</updated>
  <generator build="4464e07e99dad5532f25c08d83b3af6675536bdf" version="20230907"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/fieldfilters/_new" rel="create"/>
  <link href="/services/authorization/fieldfilters/_reload" rel="_reload"/>
  <link href="/services/authorization/fieldfilters/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

GET

Retrieve details about a specific field filter. To use GET with this endpoint, you must be a member of the admin, sc_admin, or power user role.

Request parameters

None

Response keys

"name": "A field filter name"	The name of the field filter. Field filter names can contain only alphanumeric characters and underscores (_). Spaces and special symbols are not allowed.
action.field	The name of the field to filter for this action.

action.operator	The operator for the action. Operators for actions are described as follows: - null(): Removes the field value from results of searches to which this filter is applied. - sha256(): Computes and returns the secure hash of the value of the field based on the FIPS-compliant SHA-256 (SHA-2 family) hash function. This hash is then used to replace the value of the field wherever it appears in results of searches to which this filter is applied. See Cryptographic functions in the Splunk Cloud Platform *Search Reference*. - sha512(): Computes and returns the secure hash of the value of the field based on the FIPS-compliant SHA-512 (SHA-2 family) hash function. This hash is then used to replace the value of the field wherever it appears in results of searches to which this filter is applied. See Cryptographic functions in the Splunk Cloud Platform *Search Reference*. - <string literal>: Replaces the fieldname value with the specified string wherever the field value appears in results of searches to which this filter is applied. A string literal is a sequence of characters enclosed in double quotation marks (" "). Use backslash (\ ) to escape the \ and " characters in a string literal. For example, use \\ and \" . - sed(<string literal>): For _raw fields. The sed expression acts on searches to which this filter is applied. The sed expression replaces strings in search results that are matched by a regular expression (s) or transliterates characters found in search results with corresponding characters provided by the sed expression (y). A string literal is a sequence of characters enclosed in double quotation marks (" "). Use backslash (\ ) to escape the \ and " characters in a string literal. For example, use \\ and \" .
"description": "A field filter description"	Stores a description of the field filter.
"index": "One or more index names"	Specifies an index name or a list of comma-separated index names of the target indexes you want to search that contain the data you want to protect. If an index is not specified, all indexes are searched.
limit.key	The key for the field filter limit, which limits the field filter to events with a specific target host, source, or sourcetype. You can specify only one value. If the limit key is empty, the field filter doesn't apply to events with a specific host, source, or sourcetype. Limit statements that include wildcards or the following operators are not supported: AND, OR.
limit.value	The value for the limit, which is a sequence of characters enclosed in double quotation marks (") that represents the name of one or more hosts, sources, or source types. The limit value can be a value or a list of comma-separated values for the specified limit.
"roleExemptions": [*list of exempted roles]*	A list of field filters from which each role is exempt. If a role is exempt from a field filter, the field filter is not run at search time for any users holding this role. Roles inherit all field filter exemptions from imported roles. You can't remove inherited field filter exemptions.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8106/services/authorization/fieldfilters/demo_hash_filter
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .-->
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>fieldfilters</title>
  <id>https://localhost:8106/services/authorization/fieldfilters</id>
  <updated>2023-09-07T22:14:08+00:00</updated>
  <generator build="4464e07e99dad5532f25c08d83b3af6675536bdf" version="20230907"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/fieldfilters/_new" rel="create"/>
  <link href="/services/authorization/fieldfilters/_reload" rel="_reload"/>
  <link href="/services/authorization/fieldfilters/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>demo_hash_filter</title>
    <id>https://localhost:8106/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="list"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="edit"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter" rel="remove"/>
    <link href="/servicesNS/nobody/system/authorization/fieldfilters/demo_hash_filter/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action">
          <s:dict>
            <s:key name="field">fieldName</s:key>
            <s:key name="operator">sha256()</s:key>
          </s:dict>
        </s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
```

```
         <s:list>
          <s:item>*</s:item>
         </s:list>
        </s:key>
       </s:dict>
      </s:key>
      <s:key name="removable">1</s:key>
      <s:key name="sharing">system</s:key>
     </s:dict>
    </s:key>
    <s:key name="eai:attributes">
     <s:dict>
      <s:key name="optionalFields">
       <s:list/>
      </s:key>
      <s:key name="requiredFields">
       <s:list/>
      </s:key>
      <s:key name="wildcardFields">
       <s:list>
        <s:item>.*</s:item>
       </s:list>
      </s:key>
     </s:dict>
    </s:key>
    <s:key name="limit"/>
    <s:key name="roleExemptions">
     <s:list/>
    </s:key>
   </s:dict>
  </content>
 </entry>
</feed>
```

POST

Update the specified field filter with the field values provided. To use POST with this endpoint, you must be a member of the admin or sc_admin role.

Request parameters

Name	Description
action.field	The name of the field to filter for this action. Only one field can be specified per request.
action.operator	The operator for the action. Operators for actions are described as follows: • null(): Removes the field value from results of searches to which this filter is applied. • sha256(): Computes and returns the secure hash of the value of the field based on the FIPS-compliant SHA-256 (SHA-2 family) hash function. This hash is then used to replace the value of the field wherever it appears in results of searches to which this filter is applied. See Cryptographic functions in the Splunk Cloud Platform *Search Reference*. • sha512(): Computes and returns the secure hash of the value of the field based on the FIPS-compliant SHA-512 (SHA-2 family) hash function. This hash is then used to replace the value of the field wherever it appears in results of searches to which this filter is applied. See Cryptographic functions in the Splunk Cloud Platform *Search Reference*.

Name	Description
	• <string literal>: Replaces the fieldname value with the specified string wherever the field value appears in results of searches to which this filter is applied. A string literal is a sequence of characters enclosed in double quotation marks (" "). Use backslash (\ ) to escape the \ and " characters in a string literal. For example, use \\ and \" . • sed(<string literal>): For _raw fields. The sed expression acts on searches to which this filter is applied. The sed expression replaces strings in search results that are matched by a regular expression (s) or transliterates characters found in search results with corresponding characters provided by the sed expression (y). A string literal is a sequence of characters enclosed in double quotation marks (" "). Use backslash (\ ) to escape the \ and " characters in a string literal. For example, use \\ and \" .
description = <string>	Stores a description of the field filter.
"index": "One or more index names"	Specifies an index name or a list of comma-separated index names of the target indexes you want to search that contain the data you want to protect. If an index is not specified, all indexes are searched.
limit.key	The key for the field filter limit, which limits the field filter to events with a specific target host, source, or sourcetype. You can specify only one value. If the limit key is empty, the field filter doesn't apply to events with a specific host, source, or sourcetype. Limit statements that include wildcards or the following operators are not supported: AND, OR.
limit.value	The value for the limit, which is a sequence of characters enclosed in double quotation marks (") that represents the name of one or more hosts, sources, or source types. The limit value can be a value or a list of comma-separated values for the specified limit.
"roleExemptions": [*list of exempted roles]*	A list of field filters from which each role is exempt. If a role is exempt from a field filter, the field filter is not run at search time for any users holding this role. Roles inherit all field filter exemptions from imported roles. You can't remove inherited field filter exemptions.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8106/services/authorization/fieldfilters/demo_hash_filter -d
limit=host::abc
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>fieldfilters</title>
  <id>https://localhost:8106/services/authorization/fieldfilters</id>
  <updated>2023-09-07T22:17:00+00:00</updated>
  <generator build="4464e07e99dad5532f25c08d83b3af6675536bdf" version="20230907"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/fieldfilters/_new" rel="create"/>
  <link href="/services/authorization/fieldfilters/_reload" rel="_reload"/>
  <link href="/services/authorization/fieldfilters/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>demo_hash_filter</title>
    <id>https://localhost:8106/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter" rel="list"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter" rel="edit"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter" rel="remove"/>
    <link href="/servicesNS/nobody/search/authorization/fieldfilters/demo_hash_filter/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action">
          <s:dict>
            <s:key name="field">fieldName</s:key>
            <s:key name="operator">sha256()</s:key>
          </s:dict>
        </s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="limit">
          <s:dict>
            <s:key name="key">host</s:key>
            <s:key name="value">abc</s:key>
          </s:dict>
        </s:key>
        <s:key name="roleExemptions">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

authorization/grantable_capabilities

`https://<host>:<mPort>/services/authorization/grantable_capabilities`

Get a list of all capabilities that the current user can grant.

Authorization

Capabilities listed depend on the current user authorization. If the current user has the `edit_roles` capability, the response lists all capabilities. Otherwise, depending on the current user's `edit_user` permissions and configured `grantableRoles` in `authorize.conf`, the response lists only the capabilities that the current user can grant.

GET

List capabilities that the current user can grant.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
capabilities	For users with the `edit_roles` capability, lists all capabilities. For users with `edit_roles_grantable`, `edit_user`, and `grantableRoles`, lists only grantable capabilities.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/grantable_capabilities
```

XML Response

```
<title>grantable_capabilities</title>
```

```
  <id>https://localhost:8089/services/authorization/grantable_capabilities</id>
.
.
.
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/grantable_capabilities/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>capabilities</title>
    <id>https://localhost:8089/services/authorization/grantable_capabilities/capabilities</id>
    <updated>2015-10-06T17:44:09-07:00</updated>
    <link href="/services/authorization/grantable_capabilities/capabilities" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/grantable_capabilities/capabilities" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list>
            <s:item>accelerate_datamodel</s:item>
            <s:item>accelerate_search</s:item>
            <s:item>admin_all_objects</s:item>
            <s:item>change_authentication</s:item>
            <s:item>change_own_password</s:item>
            <s:item>delete_by_keyword</s:item>
            <s:item>edit_deployment_client</s:item>
            <s:item>edit_deployment_server</s:item>
            <s:item>edit_dist_peer</s:item>
            <s:item>edit_forwarders</s:item>
            <s:item>edit_httpauths</s:item>
            <s:item>edit_input_defaults</s:item>
            <s:item>edit_monitor</s:item>
            <s:item>edit_roles</s:item>
            <s:item>edit_roles_grantable</s:item>
            <s:item>edit_scripted</s:item>
            <s:item>edit_search_head_clustering</s:item>
            <s:item>edit_search_scheduler</s:item>
            <s:item>edit_search_server</s:item>
            <s:item>edit_server</s:item>
            <s:item>edit_sourcetypes</s:item>
            <s:item>edit_splunktcp</s:item>
            <s:item>edit_splunktcp_ssl</s:item>
            <s:item>edit_tcp</s:item>
            <s:item>edit_token_http</s:item>
            <s:item>edit_udp</s:item>
            <s:item>edit_user</s:item>
            <s:item>edit_view_html</s:item>
            <s:item>edit_web_settings</s:item>
            <s:item>embed_report</s:item>
            <s:item>get_diag</s:item>
            <s:item>get_metadata</s:item>
            <s:item>get_typeahead</s:item>
            <s:item>indexes_edit</s:item>
            <s:item>input_file</s:item>
            <s:item>license_edit</s:item>
            <s:item>license_tab</s:item>
            <s:item>license_view_warnings</s:item>
            <s:item>list_deployment_client</s:item>
            <s:item>list_deployment_server</s:item>
            <s:item>list_forwarders</s:item>
            <s:item>list_httpauths</s:item>
            <s:item>list_inputs</s:item>
            <s:item>list_introspection</s:item>
            <s:item>list_search_head_clustering</s:item>
            <s:item>list_search_scheduler</s:item>
            <s:item>output_file</s:item>
            <s:item>pattern_detect</s:item>
            <s:item>request_remote_tok</s:item>
            <s:item>rest_apps_management</s:item>
            <s:item>rest_apps_view</s:item>
            <s:item>rest_properties_get</s:item>
            <s:item>rest_properties_set</s:item>
            <s:item>restart_splunkd</s:item>
            <s:item>rtsearch</s:item>
            <s:item>run_debug_commands</s:item>
            <s:item>schedule_rtsearch</s:item>
            <s:item>schedule_search</s:item>
            <s:item>search</s:item>
            <s:item>use_file_operator</s:item>
            <s:item>web_debug</s:item>
          </s:list>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

authorization/roles

`https://<host>:<mPort>/services/authorization/roles`

Create a role or get a list of defined roles with role permissions.

For additional information, see the following resources in *Securing Splunk Enterprise*.

- About role-based user access
- List of available capabilities

GET

List all roles and the permissions for each role.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
capabilities	List of capabilities assigned to role.
cumulativeRTSrchJobsQuota	Maximum number of concurrently running real-time searches for all role members. Warning message logged when limit is reached.
cumulativeSrchJobsQuota	Maximum number of concurrently running searches for all role members. Warning message logged when limit is reached.
defaultApp	The name of the app to use as the default app for this role. A user-specific default app overrides this.
fieldFilterExemption	A list of field filters from which each role is exempt. If a role is exempt from a field filter, the field filter is not run at search time for any users holding this role. Roles inherit all field filter exemptions from imported roles. You can't remove inherited field filter exemptions.
imported_capabilities	List of capabilities assigned to role made available from imported roles.
imported_roles	List of imported roles for this role. Importing other roles imports all aspects of that role, such as capabilities and allowed indexes to search. In combining multiple roles, the effective value for each attribute is value with the broadest permissions.
imported_rtSrchJobsQuota	The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit. imported_rtSrchJObsQuota specifies the quota imported from other roles.
imported_srchDiskQuota	The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total. imported_srchDiskQuota specifies the quota for this role that have imported from other roles.
imported_srchFilter	Search string, imported from other roles, that restricts the scope of searches run by this role. Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.

Name	Description
imported_srchIndexesAllowed	A list of indexes, imported from other roles, this role has permissions to search.
imported_srchIndexesDefault	A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.
imported_srchJobsQuota	The maximum number of historical searches for this role that are imported from other roles.
imported_srchTimeWin	Maximum time span of a search, in seconds. `0` indicates searches are not limited to any specific time window. imported_srchTimeWin specifies the limit from imported roles.
rtSrchJobsQuota	The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.
srchDiskQuota	The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.
srchFilter	Search string that restricts the scope of searches run by this role. Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.
srchIndexesAllowed	A list of indexes this role has permissions to search.
srchIndexesDefault	List of search indexes that default to this role when no index is specified.
srchJobsQuota	The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.
srchTimeWin	Maximum time span of a search, in seconds. `0` indicates searches are not limited to any specific time window.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles
```

XML Response

```
.
.
.
 <title>roles</title>
 <id>https://localhost:8089/services/authorization/roles</id>
 <updated>2014-06-30T13:12:17-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authorization/roles/_new" rel="create"/>
 <opensearch:totalResults>5</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
```

```
<title>admin</title>
<id>https://localhost:8089/services/authorization/roles/admin</id>
<updated>2014-06-30T13:12:17-07:00</updated>
<link href="/services/authorization/roles/admin" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/authorization/roles/admin" rel="list"/>
<link href="/services/authorization/roles/admin" rel="edit"/>
<link href="/services/authorization/roles/admin" rel="remove"/>
<content type="text/xml">
  <s:dict>
    <s:key name="capabilities">
      <s:list>
        <s:item>accelerate_datamodel</s:item>
        <s:item>admin_all_objects</s:item>
        <s:item>change_authentication</s:item>
        <s:item>edit_deployment_client</s:item>
        <s:item>edit_deployment_server</s:item>
        <s:item>edit_dist_peer</s:item>
        <s:item>edit_forwarders</s:item>
        <s:item>edit_httpauths</s:item>
        <s:item>edit_input_defaults</s:item>
        <s:item>edit_monitor</s:item>
        <s:item>edit_roles</s:item>
        <s:item>edit_scripted</s:item>
        <s:item>edit_search_server</s:item>
        <s:item>edit_server</s:item>
        <s:item>edit_splunktcp</s:item>
        <s:item>edit_splunktcp_ssl</s:item>
        <s:item>edit_tcp</s:item>
        <s:item>edit_udp</s:item>
        <s:item>edit_user</s:item>
        <s:item>edit_view_html</s:item>
        <s:item>edit_web_settings</s:item>
        <s:item>edit_win_admon</s:item>
        <s:item>edit_win_eventlogs</s:item>
        <s:item>edit_win_perfmon</s:item>
        <s:item>edit_win_regmon</s:item>
        <s:item>edit_win_wmiconf</s:item>
        <s:item>get_diag</s:item>
        <s:item>indexes_edit</s:item>
        <s:item>license_edit</s:item>
        <s:item>license_tab</s:item>
        <s:item>list_deployment_client</s:item>
        <s:item>list_deployment_server</s:item>
        <s:item>list_forwarders</s:item>
        <s:item>list_httpauths</s:item>
        <s:item>list_pdfserver</s:item>
        <s:item>list_win_localavailablelogs</s:item>
        <s:item>rest_apps_management</s:item>
        <s:item>restart_splunkd</s:item>
        <s:item>run_debug_commands</s:item>
        <s:item>write_pdfserver</s:item>
      </s:list>
    </s:key>
    <s:key name="cumulativeRTSrchJobsQuota">400</s:key>
    <s:key name="cumulativeSrchJobsQuota">200</s:key>
    <s:key name="defaultApp"></s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">system</s:key>
  </s:dict>
</s:key>
<s:key name="imported_capabilities">
  <s:list>
    <s:item>accelerate_search</s:item>
    <s:item>change_own_password</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>input_file</s:item>
    <s:item>list_inputs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>rtsearch</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
  </s:list>
</s:key>
<s:key name="imported_roles">
  <s:list>
    <s:item>power</s:item>
    <s:item>user</s:item>
  </s:list>
</s:key>
<s:key name="imported_rtSrchJobsQuota">20</s:key>
<s:key name="imported_srchDiskQuota">500</s:key>
<s:key name="imported_srchFilter"></s:key>
<s:key name="imported_srchIndexesAllowed">
  <s:list>
    <s:item>*</s:item>
  </s:list>
</s:key>
<s:key name="imported_srchIndexesDefault">
  <s:list>
    <s:item>main</s:item>
  </s:list>
</s:key>
<s:key name="imported_srchJobsQuota">10</s:key>
```

```
      <s:key name="imported_srchTimeWin">-1</s:key>
      <s:key name="rtSrchJobsQuota">100</s:key>
      <s:key name="srchDiskQuota">10000</s:key>
      <s:key name="srchFilter">*</s:key>
      <s:key name="srchIndexesAllowed">
        <s:list>
          <s:item>*</s:item>
          <s:item>_*</s:item>
        </s:list>
      </s:key>
      <s:key name="srchIndexesDefault">
        <s:list>
          <s:item>main</s:item>
          <s:item>os</s:item>
        </s:list>
      </s:key>
      <s:key name="srchJobsQuota">50</s:key>
      <s:key name="srchTimeWin">0</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>can_delete</title>
  <id>https://localhost:8089/services/authorization/roles/can_delete</id>
  <updated>2014-06-30T13:12:17-07:00</updated>
  <link href="/services/authorization/roles/can_delete" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/roles/can_delete" rel="list"/>
  <link href="/services/authorization/roles/can_delete" rel="edit"/>
  <link href="/services/authorization/roles/can_delete" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>delete_by_keyword</s:item>
          <s:item>schedule_rtsearch</s:item>
        </s:list>
      </s:key>
      <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
      <s:key name="cumulativeSrchJobsQuota">0</s:key>
      <s:key name="defaultApp"></s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="imported_capabilities">
        <s:list/>
      </s:key>
      <s:key name="imported_roles">
        <s:list/>
      </s:key>
      <s:key name="imported_rtSrchJobsQuota">0</s:key>
      <s:key name="imported_srchDiskQuota">0</s:key>
      <s:key name="imported_srchFilter"></s:key>
      <s:key name="imported_srchIndexesAllowed">
        <s:list/>
      </s:key>
      <s:key name="imported_srchIndexesDefault">
        <s:list/>
      </s:key>
      <s:key name="imported_srchJobsQuota">0</s:key>
      <s:key name="imported_srchTimeWin">-1</s:key>
      <s:key name="rtSrchJobsQuota">6</s:key>
      <s:key name="srchDiskQuota">100</s:key>
      <s:key name="srchFilter"></s:key>
      <s:key name="srchIndexesAllowed">
        <s:list/>
      </s:key>
      <s:key name="srchIndexesDefault">
        <s:list/>
      </s:key>
      <s:key name="srchJobsQuota">3</s:key>
      <s:key name="srchTimeWin">-1</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>power</title>
  <id>https://localhost:8089/services/authorization/roles/power</id>
  <updated>2014-06-30T13:12:17-07:00</updated>
  <link href="/services/authorization/roles/power" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/roles/power" rel="list"/>
  <link href="/services/authorization/roles/power" rel="edit"/>
  <link href="/services/authorization/roles/power" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>embed_report</s:item>
          <s:item>rtsearch</s:item>
          <s:item>schedule_search</s:item>
        </s:list>
      </s:key>
      <s:key name="cumulativeRTSrchJobsQuota">200</s:key>
      <s:key name="cumulativeSrchJobsQuota">100</s:key>
      <s:key name="defaultApp"></s:key>
      <s:key name="eai:acl">
        <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">system</s:key>
  </s:dict>
</s:key>
<s:key name="imported_capabilities">
  <s:list>
    <s:item>accelerate_search</s:item>
    <s:item>change_own_password</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>input_file</s:item>
    <s:item>list_inputs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>search</s:item>
  </s:list>
</s:key>
<s:key name="imported_roles">
  <s:list>
    <s:item>user</s:item>
  </s:list>
</s:key>
<s:key name="imported_rtSrchJobsQuota">6</s:key>
<s:key name="imported_srchDiskQuota">100</s:key>
<s:key name="imported_srchFilter"></s:key>
<s:key name="imported_srchIndexesAllowed">
  <s:list>
    <s:item>*</s:item>
  </s:list>
</s:key>
<s:key name="imported_srchIndexesDefault">
  <s:list>
    <s:item>main</s:item>
  </s:list>
</s:key>
<s:key name="imported_srchJobsQuota">3</s:key>
<s:key name="imported_srchTimeWin">-1</s:key>
<s:key name="rtSrchJobsQuota">20</s:key>
<s:key name="srchDiskQuota">500</s:key>
```

```
        <s:key name="srchFilter"></s:key>
        <s:key name="srchIndexesAllowed">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="srchIndexesDefault">
          <s:list>
            <s:item>main</s:item>
          </s:list>
        </s:key>
        <s:key name="srchJobsQuota">10</s:key>
        <s:key name="srchTimeWin">-1</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>splunk-system-role</title>
    <id>https://localhost:8089/services/authorization/roles/splunk-system-role</id>
    <updated>2014-06-30T13:12:17-07:00</updated>
    <link href="/services/authorization/roles/splunk-system-role" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/roles/splunk-system-role" rel="list"/>
    <link href="/services/authorization/roles/splunk-system-role" rel="edit"/>
    <link href="/services/authorization/roles/splunk-system-role" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list/>
        </s:key>
        <s:key name="cumulativeRTSrchJobsQuota">100</s:key>
        <s:key name="cumulativeSrchJobsQuota">50</s:key>
        <s:key name="defaultApp"></s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="imported_capabilities">
          <s:list>
    <s:item>accelerate_datamodel</s:item>
    <s:item>accelerate_search</s:item>
    <s:item>admin_all_objects</s:item>
    <s:item>change_authentication</s:item>
    <s:item>change_own_password</s:item>
    <s:item>edit_deployment_client</s:item>
    <s:item>edit_deployment_server</s:item>
    <s:item>edit_dist_peer</s:item>
    <s:item>edit_forwarders</s:item>
    <s:item>edit_httpauths</s:item>
    <s:item>edit_input_defaults</s:item>
    <s:item>edit_monitor</s:item>
    <s:item>edit_roles</s:item>
    <s:item>edit_scripted</s:item>
    <s:item>edit_search_server</s:item>
    <s:item>edit_server</s:item>
    <s:item>edit_splunktcp</s:item>
    <s:item>edit_splunktcp_ssl</s:item>
    <s:item>edit_tcp</s:item>
    <s:item>edit_udp</s:item>
    <s:item>edit_user</s:item>
    <s:item>edit_view_html</s:item>
    <s:item>edit_web_settings</s:item>
    <s:item>edit_win_admon</s:item>
    <s:item>edit_win_eventlogs</s:item>
    <s:item>edit_win_perfmon</s:item>
    <s:item>edit_win_regmon</s:item>
    <s:item>edit_win_wmiconf</s:item>
    <s:item>embed_report</s:item>
    <s:item>get_diag</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>indexes_edit</s:item>
    <s:item>input_file</s:item>
    <s:item>license_edit</s:item>
    <s:item>license_tab</s:item>
    <s:item>list_deployment_client</s:item>
    <s:item>list_deployment_server</s:item>
    <s:item>list_forwarders</s:item>
    <s:item>list_httpauths</s:item>
    <s:item>list_inputs</s:item>
    <s:item>list_pdfserver</s:item>
    <s:item>list_win_localavailablelogs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_management</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>restart_splunkd</s:item>
    <s:item>rtsearch</s:item>
    <s:item>run_debug_commands</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>schedule_search</s:item>
    <s:item>search</s:item>
    <s:item>write_pdfserver</s:item>
  </s:list>
</s:key>
<s:key name="imported_roles">
  <s:list>
    <s:item>admin</s:item>
  </s:list>
```

```
        </s:key>
        <s:key name="imported_rtSrchJobsQuota">100</s:key>
        <s:key name="imported_srchDiskQuota">10000</s:key>
        <s:key name="imported_srchFilter">*</s:key>
        <s:key name="imported_srchIndexesAllowed">
          <s:list>
            <s:item>*</s:item>
            <s:item>_*</s:item>
          </s:list>
        </s:key>
        <s:key name="imported_srchIndexesDefault">
          <s:list>
            <s:item>main</s:item>
            <s:item>os</s:item>
          </s:list>
        </s:key>
        <s:key name="imported_srchJobsQuota">50</s:key>
        <s:key name="imported_srchTimeWin">-1</s:key>
        <s:key name="rtSrchJobsQuota">6</s:key>
        <s:key name="srchDiskQuota">100</s:key>
        <s:key name="srchFilter"></s:key>
        <s:key name="srchIndexesAllowed">
          <s:list/>
        </s:key>
        <s:key name="srchIndexesDefault">
          <s:list/>
        </s:key>
        <s:key name="srchJobsQuota">3</s:key>
        <s:key name="srchTimeWin">-1</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>user</title>
    <id>https://localhost:8089/services/authorization/roles/user</id>
    <updated>2014-06-30T13:12:17-07:00</updated>
    <link href="/services/authorization/roles/user" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/roles/user" rel="list"/>
    <link href="/services/authorization/roles/user" rel="edit"/>
    <link href="/services/authorization/roles/user" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list>
            <s:item>accelerate_search</s:item>
            <s:item>change_own_password</s:item>
            <s:item>get_metadata</s:item>
            <s:item>get_typeahead</s:item>
            <s:item>input_file</s:item>
            <s:item>list_inputs</s:item>
            <s:item>output_file</s:item>
            <s:item>request_remote_tok</s:item>
            <s:item>rest_apps_view</s:item>
            <s:item>rest_properties_get</s:item>
            <s:item>rest_properties_set</s:item>
            <s:item>schedule_rtsearch</s:item>
            <s:item>search</s:item>
          </s:list>
        </s:key>
        <s:key name="cumulativeRTSrchJobsQuota">100</s:key>
        <s:key name="cumulativeSrchJobsQuota">50</s:key>
        <s:key name="defaultApp"></s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="imported_capabilities">
          <s:list/>
        </s:key>
        <s:key name="imported_roles">
          <s:list/>
        </s:key>
        <s:key name="imported_rtSrchJobsQuota">0</s:key>
        <s:key name="imported_srchDiskQuota">0</s:key>
        <s:key name="imported_srchFilter"></s:key>
        <s:key name="imported_srchIndexesAllowed">
          <s:list/>
        </s:key>
        <s:key name="imported_srchIndexesDefault">
          <s:list/>
        </s:key>
        <s:key name="imported_srchJobsQuota">0</s:key>
        <s:key name="imported_srchTimeWin">-1</s:key>
        <s:key name="rtSrchJobsQuota">6</s:key>
        <s:key name="srchDiskQuota">100</s:key>
        <s:key name="srchFilter"></s:key>
        <s:key name="srchIndexesAllowed">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="srchIndexesDefault">
          <s:list>
            <s:item>main</s:item>
          </s:list>
        </s:key>
        <s:key name="srchJobsQuota">3</s:key>
        <s:key name="srchTimeWin">-1</s:key>
      </s:dict>
    </content>
```

```
</entry>
```

POST

Create a user role.

Request parameters

Name	Type	Description
capabilities	String	List of capabilities assigned to role. To send multiple capabilities, send this argument multiple times. Roles inherit all capabilities from imported roles.
cumulativeRTSrchJobsQuota	Number	Maximum number of concurrently running real-time searches that all members of this role can have. *Note*: If a user belongs to multiple roles then the user first consumes searches from the roles with the largest cumulative search quota. When the quota of a role is completely used up then roles with lower quotas are examined.
cumulativeSrchJobsQuota	Number	Maximum number of concurrently running searches for all role members. Warning message logged when limit is reached. *Note*: If a user belongs to multiple roles then the user first consumes searches from the roles with the largest cumulative search quota. When the quota of a role is completely used up then roles with lower quotas are examined.
defaultApp	String	Specify the folder name of the default app to use for this role. A user-specific default app overrides this.
imported_roles	String	Specify a role to import attributes from. To import multiple roles, specify them separately. By default a role imports no other roles. Importing other roles imports all aspects of that role, such as capabilities and allowed indexes to search. In combining multiple roles, the effective value for each attribute is the value with the broadest permissions. Default roles • admin • can_delete • power • user You can specify additional roles created.
name required	String	**Required**. The name of the user role to create.
rtSrchJobsQuota	Number	Specify the maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.
srchDiskQuota	Number	Specifies the maximum disk space in MB that can be used by a user's search jobs. For example, a value of `100` limits this role to 100 MB total.
srchFilter	String	

Name	Type	Description
		Specify a search string that restricts the scope of searches run by this role. Search results for this role only show events that also match the search string you specify. In the case that a user has multiple roles with different search filters, they are combined with an OR. The search string can include search fields and the following terms. • `source` • `host` • `index` • `eventtype` • `sourcetype` • `*` • `OR` • `AND` Example: `"host=web* OR source=/var/log/*"` **Note:** You can also use the *srchIndexesAllowed* and *srchIndexesDefault* parameters to limit the search on indexes.
srchIndexesAllowed	String	Index that this role has permissions to search. Pass this argument once for each index that you want to specify. These may be wildcarded, but the index name must begin with an underscore to match internal indexes. Search indexes available by default include the following. • All internal indexes • All non-internal indexes • _audit • _blocksignature • _internal • _thefishbucket • history • main You can also specify other search indexes added to the server.
srchIndexesDefault	String	For this role, indexes to search when no index is specified. These indexes can be wildcarded, with the exception that '*' does not match internal indexes. To match internal indexes, start with '_'. All internal indexes are represented by '_*'. A user with this role can search other indexes using "index= " For example, "index=special_index". Search indexes available by default include the following. • All internal indexes • All non-internal indexes • _audit • _blocksignature • _internal • _thefishbucket • history

Name	Type	Description
		- main - other search indexes added to the server
srchJobsQuota	Number	The maximum number of concurrent searches a user with this role is allowed to run. For users with multiple roles, the maximum quota value among all of the roles applies.
srchTimeWin	Number	Maximum time span of a search, in seconds. By default, searches are not limited to any specific time window. To override any search time windows from imported roles, set srchTimeWin to '0', as the 'admin' role does.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles -d name=newrole1 -d
imported_roles=user
```

XML Response

```
.
.
.
<title>roles</title>
 <id>https://localhost:8089/services/authorization/roles</id>
 <updated>2014-06-30T13:21:50-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/authorization/roles/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>newrole1</title>
   <id>https://localhost:8089/services/authorization/roles/newrole1</id>
   <updated>2014-06-30T13:21:50-07:00</updated>
   <link href="/services/authorization/roles/newrole1" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/authorization/roles/newrole1" rel="list"/>
   <link href="/services/authorization/roles/newrole1" rel="edit"/>
   <link href="/services/authorization/roles/newrole1" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capabilities">
         <s:list/>
       </s:key>
       <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
       <s:key name="cumulativeSrchJobsQuota">0</s:key>
```

```
<s:key name="defaultApp"></s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>admin</s:item>
            <s:item>splunk-system-role</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>admin</s:item>
            <s:item>splunk-system-role</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">system</s:key>
  </s:dict>
</s:key>
<s:key name="imported_capabilities">
  <s:list>
    <s:item>accelerate_search</s:item>
    <s:item>change_own_password</s:item>
    <s:item>get_metadata</s:item>
    <s:item>get_typeahead</s:item>
    <s:item>input_file</s:item>
    <s:item>list_inputs</s:item>
    <s:item>output_file</s:item>
    <s:item>request_remote_tok</s:item>
    <s:item>rest_apps_view</s:item>
    <s:item>rest_properties_get</s:item>
    <s:item>rest_properties_set</s:item>
    <s:item>schedule_rtsearch</s:item>
    <s:item>search</s:item>
  </s:list>
</s:key>
<s:key name="imported_roles">
  <s:list>
    <s:item>user</s:item>
  </s:list>
</s:key>
<s:key name="imported_rtSrchJobsQuota">6</s:key>
<s:key name="imported_srchDiskQuota">100</s:key>
<s:key name="imported_srchFilter"></s:key>
<s:key name="imported_srchIndexesAllowed">
  <s:list>
    <s:item>*</s:item>
  </s:list>
</s:key>
<s:key name="imported_srchIndexesDefault">
  <s:list>
    <s:item>main</s:item>
  </s:list>
```

```
      </s:key>
      <s:key name="imported_srchJobsQuota">3</s:key>
      <s:key name="imported_srchTimeWin">-1</s:key>
      <s:key name="rtSrchJobsQuota">6</s:key>
      <s:key name="srchDiskQuota">100</s:key>
      <s:key name="srchFilter"></s:key>
      <s:key name="srchIndexesAllowed">
        <s:list/>
      </s:key>
      <s:key name="srchIndexesDefault">
        <s:list/>
      </s:key>
      <s:key name="srchJobsQuota">3</s:key>
      <s:key name="srchTimeWin">-1</s:key>
    </s:dict>
  </content>
</entry>
```

authorization/roles/{name}

`https://<host>:<mPort>/services/authorization/roles/<name>`

Access, create, or delete properties for the `{name}` role.

For additional information, see the List of available capabilities in *Securing Splunk Enterprise*.

DELETE

Delete the specified role.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/authorization/roles/newrole1
```

XML Response

```
.
.
.
<title>roles</title>
 <id>https://localhost:8089/services/authorization/roles</id>
 <updated>2014-06-30T13:21:50-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
```

```
</author>
<link href="/services/authorization/roles/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>newrole1</title>
  <id>https://localhost:8089/services/authorization/roles/newrole1</id>
  <updated>2014-06-30T13:21:50-07:00</updated>
  <link href="/services/authorization/roles/newrole1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/roles/newrole1" rel="list"/>
  <link href="/services/authorization/roles/newrole1" rel="edit"/>
  <link href="/services/authorization/roles/newrole1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list/>
      </s:key>
      <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
      <s:key name="cumulativeSrchJobsQuota">0</s:key>
      <s:key name="defaultApp"></s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="imported_capabilities">
        <s:list>
          <s:item>accelerate_search</s:item>
          <s:item>change_own_password</s:item>
          <s:item>get_metadata</s:item>
          <s:item>get_typeahead</s:item>
          <s:item>input_file</s:item>
          <s:item>list_inputs</s:item>
          <s:item>output_file</s:item>
          <s:item>request_remote_tok</s:item>
```

```
           <s:item>rest_apps_view</s:item>
           <s:item>rest_properties_get</s:item>
           <s:item>rest_properties_set</s:item>
           <s:item>schedule_rtsearch</s:item>
           <s:item>search</s:item>
         </s:list>
       </s:key>
       <s:key name="imported_roles">
         <s:list>
           <s:item>user</s:item>
         </s:list>
       </s:key>
       <s:key name="imported_rtSrchJobsQuota">6</s:key>
       <s:key name="imported_srchDiskQuota">100</s:key>
       <s:key name="imported_srchFilter"></s:key>
       <s:key name="imported_srchIndexesAllowed">
         <s:list>
           <s:item>*</s:item>
         </s:list>
       </s:key>
       <s:key name="imported_srchIndexesDefault">
         <s:list>
           <s:item>main</s:item>
         </s:list>
       </s:key>
       <s:key name="imported_srchJobsQuota">3</s:key>
       <s:key name="imported_srchTimeWin">-1</s:key>
       <s:key name="rtSrchJobsQuota">6</s:key>
       <s:key name="srchDiskQuota">100</s:key>
       <s:key name="srchFilter"></s:key>
       <s:key name="srchIndexesAllowed">
         <s:list/>
       </s:key>
       <s:key name="srchIndexesDefault">
         <s:list/>
       </s:key>
       <s:key name="srchJobsQuota">3</s:key>
       <s:key name="srchTimeWin">-1</s:key>
     </s:dict>
   </content>
 </entry>
```

GET

Access the specified role.

Request parameters

None

Response keys

Name	Description
capabilities	List of capabilities assigned to this role.
cumulativeRTSrchJobsQuota	Maximum number of concurrently running real-time searches for all role members. A warning message is logged when this limit is reached.
cumulativeSrchJobsQuota	Maximum number of concurrently running searches for all role members. A warning message is logged when this limit is reached.

Name	Description
defaultApp	The name of the app to use as the default app for this role. A user-specific default app overrides this.
fieldFilterExemption	A list of field filters from which this role is exempt. If a role is exempt from a field filter, the field filter is not run at search time for any users holding this role. Roles inherit all field filter exemptions from imported roles. You can't remove inherited field filter exemptions.
imported_capabilities	List of capabilities assigned to the role that were made available from imported roles.
imported_roles	List of imported roles for this role. Importing other roles imports all aspects of that role, such as capabilities and allowed indexes to search. In combining multiple roles, the effective value for each attribute is value with the broadest permissions.
imported_rtSrchJobsQuota	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit. *imported_rtSrchJObsQuota* specifies the quota imported from other roles.
imported_srchDiskQuota	The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total. *imported_rtSrchJObsQuota* specifies the quota imported from other roles.
imported_srchFilter	Search string, imported from other roles, that restricts the scope of searches run by this role. Search results for this role show only events that also match this search string. When a user has multiple roles with different search filters, they are combined with an `OR`.
imported_srchIndexesAllowed	A list of indexes, imported from other roles, that this role has permissions to search.
imported_srchIndexesDefault	A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.
imported_srchJobsQuota	The maximum number of historical searches for this role that are imported from other roles.
imported_srchTimeWin	Maximum time span of a search, in seconds. `0` indicates searches are not limited to any specific time window. *imported_srchTimeWin* specifies the limit from imported roles.
rtSrchJobsQuota	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.
srchDiskQuota	The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.
srchFilter	Search string that restricts the scope of searches run by this role. Search results for this role show only events that also match this search string. When a user has multiple roles with different search filters, they are combined with an `OR`.
srchIndexesAllowed	A list of indexes this role has permissions to search.
srchIndexesDefault	List of search indexes that default to this role when no index is specified.
srchIndexesDisallowed	A list of indexes that this role does not have permission to search on or delete.

Name	Description
srchJobsQuota	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.
srchTimeWin	Maximum time span of a search, in seconds. `0` indicates searches are not limited to any specific time window.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles/user
```

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles/user
```

XML Response

```
    <title>user</title>
    <id>/services/authorization/roles/user</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/authorization/roles/user" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/roles/user" rel="list"/>
    <link href="/services/authorization/roles/user" rel="edit"/>
    <link href="/services/authorization/roles/user" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list>
            <s:item>change_own_password</s:item>
            <s:item>get_metadata</s:item>
            <s:item>get_typeahead</s:item>
            <s:item>list_inputs</s:item>
            <s:item>list_tokens_own</s:item>
            <s:item>request_remote_tok</s:item>
            <s:item>rest_apps_view</s:item>
            <s:item>rest_properties_get</s:item>
            <s:item>rest_properties_set</s:item>
            <s:item>search</s:item>
          </s:list>
        </s:key>
        <s:key name="cumulativeRTSrchJobsQuota">20</s:key>
        <s:key name="cumulativeSrchJobsQuota">10</s:key>
        <s:key name="defaultApp"></s:key>
        <s:key name="deleteIndexesAllowed">
          <s:list/>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>capabilities</s:item>
                <s:item>cumulativeRTSrchJobsQuota</s:item>
                <s:item>cumulativeSrchJobsQuota</s:item>
                <s:item>defaultApp</s:item>
                <s:item>deleteIndexesAllowed</s:item>
                <s:item>federatedProviders</s:item>
                <s:item>fieldFilterLimit</s:item>
                <s:item>grantable_roles</s:item>
                <s:item>imported_roles</s:item>
                <s:item>rtSrchJobsQuota</s:item>
                <s:item>srchDiskQuota</s:item>
                <s:item>srchFilter</s:item>
                <s:item>srchIndexesAllowed</s:item>
                <s:item>srchIndexesDefault</s:item>
                <s:item>srchIndexesDisallowed</s:item>
                <s:item>srchJobsQuota</s:item>
                <s:item>srchTimeEarliest</s:item>
                <s:item>srchTimeWin</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>fieldFilter\-.*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="fieldFilter-bar">NULL</s:key>
        <s:key name="fieldFilter-foo">sha256</s:key>
        <s:key name="fieldFilterLimit">sourcetype::foobar</s:key>
        <s:key name="grantable_roles">
          <s:list/>
        </s:key>
        <s:key name="imported_capabilities">
          <s:list/>
```

```
        </s:key>
        <s:key name="imported_roles">
          <s:list/>
        </s:key>
        <s:key name="imported_rtSrchJobsQuota">0</s:key>
        <s:key name="imported_srchDiskQuota">0</s:key>
        <s:key name="imported_srchFilter"></s:key>
        <s:key name="imported_srchIndexesAllowed">
          <s:list/>
        </s:key>
        <s:key name="imported_srchIndexesDefault">
          <s:list/>
        </s:key>
        <s:key name="imported_srchIndexesDisallowed">
          <s:list/>
        </s:key>
        <s:key name="imported_srchJobsQuota">0</s:key>
        <s:key name="imported_srchTimeEarliest">-1</s:key>
        <s:key name="imported_srchTimeWin">-1</s:key>
        <s:key name="rtSrchJobsQuota">17</s:key>
        <s:key name="srchDiskQuota">100</s:key>
        <s:key name="srchFilter"></s:key>
        <s:key name="srchIndexesAllowed">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="srchIndexesDefault">
          <s:list>
            <s:item>main</s:item>
          </s:list>
        </s:key>
        <s:key name="srchIndexesDisallowed">
          <s:list/>
        </s:key>
        <s:key name="srchJobsQuota">16</s:key>
        <s:key name="srchTimeEarliest">-1</s:key>
        <s:key name="srchTimeWin">-1</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update the specified role.

Request parameters

Name	Type	Description
capabilities	String	List of capabilities assigned to this role.
cumulativeRTSrchJobsQuota	Number	Maximum number of concurrently running real-time searches for all role members. A warning message is logged when this limit is reached.
cumulativeSrchJobsQuota	Number	Maximum number of concurrently running searches for all role members. A warning message is logged when this limit is reached.
defaultApp	String	The folder name for the app to use as the default app for this role. A user-specific default app overrides this.

Name	Type	Description
imported_capabilities	String	List of capabilities assigned to the role that were made available from imported roles.
imported_roles	String	Add an imported role one at a time. Importing other roles imports all aspects of that role, such as capabilities and allowed indexes to search. In combining multiple roles, the effective value for each attribute is value with the broadest permissions.
imported_rtSrchJobsQuota	String	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit. *imported_rtSrchJObsQuota* specifies the quota imported from other roles.
imported_srchDiskQuota	String	The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total. *imported_rtSrchJObsQuota* specifies the quota imported from other roles.
imported_srchFilter	String	Search string, imported from other roles, that restricts the scope of searches run by this role. Search results for this role show only events that also match this search string. When a user has multiple roles with different search filters, they are combined with an `OR`.
imported_srchIndexesAllowed	String	A list of indexes, imported from other roles, that this role has permissions to search.
imported_srchIndexesDefault	String	A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.
imported_srchJobsQuota	String	The maximum number of historical searches for this role that are imported from other roles.
imported_srchTimeWin	String	Maximum time span of a search, in seconds. `0` indicates searches are not limited to any specific time window. *imported_srchTimeWin* specifies the limit from imported roles.
rtSrchJobsQuota	Number	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.
srchDiskQuota	Number	The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.
srchFilter	String	Search string that restricts the scope of searches run by this role. Search results for this role show only events that also match this search string. When a user has multiple roles with different search filters, they are combined with an `OR`.
srchIndexesAllowed	String	A list of indexes this role has permissions to search.
srchIndexesDefault	String	List of search indexes that default to this role when no index is specified.
srchIndexesDisallowed	String	A list of indexes that this role does not have permission to search on or delete.
srchJobsQuota	Number	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.

Name	Type	Description
srchTimeWin	Number	Maximum time span of a search, in seconds. `0` indicates searches are not limited to any specific time window.

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/users/user
fieldFilter-foo=sha256&fieldFilter-bar=NULL&fieldFilterLimit=sourcetype::foobar
```

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles/newrole1 -d
defaultApp=launcher
```

XML Response

```
 <title>roles</title>
  <id>/services/authorization/roles</id>
  <updated>2022-01-26T15:46:33-08:00</updated>
  <generator build="c96e1830f423ed31e033be95a0703e944ae27d25" version="20220124"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/roles/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>user</title>
    <id>/services/authorization/roles/user</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/authorization/roles/user" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/roles/user" rel="list"/>
    <link href="/services/authorization/roles/user" rel="edit"/>
    <link href="/services/authorization/roles/user" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list>
            <s:item>change_own_password</s:item>
            <s:item>get_metadata</s:item>
            <s:item>get_typeahead</s:item>
            <s:item>list_inputs</s:item>
            <s:item>list_tokens_own</s:item>
            <s:item>request_remote_tok</s:item>
            <s:item>rest_apps_view</s:item>
            <s:item>rest_properties_get</s:item>
            <s:item>rest_properties_set</s:item>
            <s:item>search</s:item>
          </s:list>
        </s:key>
        <s:key name="cumulativeRTSrchJobsQuota">20</s:key>
        <s:key name="cumulativeSrchJobsQuota">10</s:key>
        <s:key name="defaultApp"></s:key>
        <s:key name="deleteIndexesAllowed">
          <s:list/>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="fieldFilter-bar">NULL</s:key>
        <s:key name="fieldFilter-foo">sha256</s:key>
        <s:key name="fieldFilterLimit">sourcetype::foobar</s:key>
        <s:key name="grantable_roles">
          <s:list/>
        </s:key>
        <s:key name="imported_capabilities">
          <s:list/>
        </s:key>
        <s:key name="imported_roles">
          <s:list/>
        </s:key>
        <s:key name="imported_rtSrchJobsQuota">0</s:key>
        <s:key name="imported_srchDiskQuota">0</s:key>
        <s:key name="imported_srchFilter"></s:key>
        <s:key name="imported_srchIndexesAllowed">
          <s:list/>
        </s:key>
        <s:key name="imported_srchIndexesDefault">
          <s:list/>
        </s:key>
        <s:key name="imported_srchIndexesDisallowed">
          <s:list/>
```

```
        </s:key>
        <s:key name="imported_srchJobsQuota">0</s:key>
        <s:key name="imported_srchTimeEarliest">-1</s:key>
        <s:key name="imported_srchTimeWin">-1</s:key>
        <s:key name="rtSrchJobsQuota">17</s:key>
        <s:key name="srchDiskQuota">100</s:key>
        <s:key name="srchFilter"></s:key>
        <s:key name="srchIndexesAllowed">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="srchIndexesDefault">
          <s:list>
            <s:item>main</s:item>
          </s:list>
        </s:key>
        <s:key name="srchIndexesDisallowed">
          <s:list/>
        </s:key>
        <s:key name="srchJobsQuota">16</s:key>
        <s:key name="srchTimeEarliest">-1</s:key>
        <s:key name="srchTimeWin">-1</s:key>
      </s:dict>
    </content>
  </entry>
```

Any Splunk roles that you create using this method will inherit a default set of capabilities. This inheritance occurs when you reload the authentication system. In search head clusters, this happens as part of configuration replication. You must manually reload the authentication system on standalone search heads for this inheritance to take effect.

authorization/tokens

`https://<host>:<mPort>/services/authorization/tokens`

Create, get information on, or modify tokens for authentication.

For additional information, see the following resources in *Securing Splunk Enterprise*.

- Set up authentication with tokens
- Create authentication tokens
- Manage or delete authentication tokens

GET

List information on tokens.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
username	The username whose tokens you want to see. Optional. If not provided, all tokens are displayed.
id	The ID of the token whose information you want to see. Optional.
status	Show only tokens of a specific status. Optional. Valid values are `enabled` or `disabled`.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/tokens
```

XML Response

```
.
.
.
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T15:04:30-07:00</updated>
  <generator build="6c6f0a269b91" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/tokens/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9</title>
    <id>https://splunkaday-linux-current:8089/services/authorization/tokens
/60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link
href="/services/authorization/tokens/60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/authorization/tokens/60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9"
rel="list"/>
    <link
href="/services/authorization/tokens/60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9"
rel="edit"/>
    <link
href="/services/authorization/tokens/60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9"
rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="claims">
          <s:dict>
            <s:key name="aud">Tokentown</s:key>
            <s:key name="exp">0</s:key>
            <s:key name="iat">1556488991</s:key>
            <s:key name="idp">splunk</s:key>
            <s:key name="iss">admin from docs-unix-4</s:key>
            <s:key name="nbr">1556488991</s:key>
            <s:key name="roles">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="sub">admin</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="headers">
          <s:dict>
            <s:key name="alg">HS512</s:key>
            <s:key name="kid">splunk.secret</s:key>
            <s:key name="ttyp">static</s:key>
            <s:key name="ver">v1</s:key>
          </s:dict>
        </s:key>
        <s:key name="lastUsed">0</s:key>
        <s:key name="lastUsedIp"></s:key>
        <s:key name="status">enabled</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Change the status of one or more tokens.

Request parameters

Name	Type	Description

Name	Type	Description
name	String	The user of the token. Can be up to 1024 characters.
audience	String	The purpose for the token. Can be up to 256 characters.
expires_on	String	The time that the token expires. Can be either of an absolute time (ex.: `2019-02-09T07:35:00+07:00`) or a relative time (ex.: `+90d`). This time cannot be in the past. *Note*: If you specify `not_before` in addition to `expires_on`, `not_before` cannot be after `expires_on`..
not_before	String	The time that the token becomes valid. Can be an absolute time or a relative time. This time cannot be in the past. *Note*: If you specify `not_before` in addition to `expires_on`, `not_before` cannot be after `expires_on`..

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/tokens -d name=user12 -d
audience=Users
```

XML Response

```
.
.
.
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T15:26:52-07:00</updated>
  <generator build="6c6f0a269b91" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/tokens/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>tokens</title>
    <id>https://splunkaday-linux-current:8089/services/authorization/tokens/tokens</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/authorization/tokens/tokens" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/tokens/tokens" rel="list"/>
    <link href="/services/authorization/tokens/tokens" rel="edit"/>
    <link href="/services/authorization/tokens/tokens" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="id">a1afa1a74528731191ab3e597889b2013c57cc301e06a9cf4e86f8282144ba09</s:key>
        <s:key
name="token"><![CDATA[eyJraWQiOiJzcGx1bmsuc2VjcmV0IiwiYWxnIjoiSFM1MTIiLCJ2ZXIiOiJ2MSIsInR0eXAiOiJzdGF0aWMifQ
.eyJpc3MiOiJhZG1pbiBmcm9tIGRvY3MtdW5peC00Iiwic3ViIjoidXNlcjEyIiwiYXVkIjoiVXNlcnMiLCJpZHAiOiJzcGx1bmsiLCJqdGkiO
iJhMWFmYTFhNzQ1Mjg3MzExOTFhYjNlNTk3ODg5YjIwMTNjNTdjYzMwMWUwNmE5Y2Y0ZTg2ZjgyODIxNDRiYTA5IiwiaWF0IjoxNTU2NDkwNDE
yLCJleHAiOjAsIm5iciI6MTU1NjQ5MDQxMn0.KQhlN5bdiEPVB_m85VV3CVIA
_Ux5CI24AHoer6iElAbGLLPrwvN0ntHsagUFyrhk6edvDofRvG6Z1o5F4NS8Cg]]></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

authorization/tokens/{name}

`https://<host>:<mPort>/services/authorization/tokens/name>`

Get information on, modify, or delete authentication tokens for the `{name}` user.

For additional information, see the following resources in *Securing Splunk Enterprise*.

- Set up authentication with tokens
- Manage or delete authentication tokens

DELETE

Delete a token for the specified user.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Description
id	The ID of the token you want to delete. Optional. If not specified, then all tokens that belong to `{username}` are deleted.

Example request and response

XML Request

```
curl -k -u admin:changeme -X DELETE https://localhost:8089/services/authorization/tokens/user12
```

XML Response

```
.
.
.
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T16:13:45-07:00</updated>
  <generator build="6c6f0a269b91" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/tokens/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Token(s), removed.</s:msg>
  </s:messages>
  <entry>
    <title>cdc2f1ddc0e240695feb977c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf</title>
    <id>https://splunkaday-linux-current:8089/services/authorization/tokens
/cdc2f1ddc0e240695feb977c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link
href="/services/authorization/tokens/cdc2f1ddc0e240695feb977c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/authorization/tokens/cdc2f1ddc0e240695feb977c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf"
rel="list"/>
    <link
href="/services/authorization/tokens/cdc2f1ddc0e240695feb977c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf"
rel="edit"/>
    <link
href="/services/authorization/tokens/cdc2f1ddc0e240695feb977c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf"
rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="claims">
          <s:dict>
            <s:key name="aud">Tokentown</s:key>
            <s:key name="exp">0</s:key>
            <s:key name="iat">1556490311</s:key>
            <s:key name="idp">splunk</s:key>
            <s:key name="iss">admin from docs-unix-4</s:key>
            <s:key name="nbr">1556490311</s:key>
            <s:key name="roles">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="sub">admin</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="headers">
          <s:dict>
            <s:key name="alg">HS512</s:key>
            <s:key name="kid">splunk.secret</s:key>
            <s:key name="ttyp">static</s:key>
            <s:key name="ver">v1</s:key>
          </s:dict>
        </s:key>
        <s:key name="lastUsed">0</s:key>
        <s:key name="lastUsedIp"></s:key>
        <s:key name="status">enabled</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a token for the specified username.

Request parameters

Name	Type	Description

name	String	The user of the token. Can be up to 1024 characters.
audience	String	The purpose for the token. Can be up to 256 characters.
expires_on	String	The time that the token expires. Can be either of an absolute time (ex.: `2019-02-09T07:35:00+07:00`) or a relative time (ex.: `+90d`). This time cannot be in the past. *Note*: If you specify `not_before` in addition to `expires_on`, `not_before` cannot be after `expires_on`..
not_before	String	The time that the token becomes valid. Can be an absolute time or a relative time. This time cannot be in the past. *Note*: If you specify `not_before` in addition to `expires_on`, `not_before` cannot be after `expires_on`..

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/tokens/user12 -d audience=Users -d
expires_on=+90d@d
```

XML Response

```
.
.
.
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T15:26:52-07:00</updated>
  <generator build="6c6f0a269b91" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/tokens/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>tokens</title>
    <id>https://splunkaday-linux-current:8089/services/authorization/tokens/tokens</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/authorization/tokens/tokens" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/tokens/tokens" rel="list"/>
    <link href="/services/authorization/tokens/tokens" rel="edit"/>
    <link href="/services/authorization/tokens/tokens" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="id">a1afa1a74528731191ab3e597889b2013c57cc301e06a9cf4e86f8282144ba09</s:key>
        <s:key
name="token"><![CDATA[eyJraWQiOiJzcGx1bmsuc2VjcmV0IiwiYWxnIjoiSFM1MTIiLCJ2ZXIiOiJ2MSIsInR0eXAiOiJzdGF0aWMifQ
.eyJpc3MiOiJhZG1pbiBmcm9tIGRvY3MtdW5peC00Iiwic3ViIjoidXNlcjEyIiwiYXVkIjoiVXNlcnMiLCJpZHAiOiJzcGx1bmsiLCJqdGkiO
iJhMWFmYTFhNzQ1Mjg3MzExOTFhYjNlNTk3ODg5YjIwMTNjNTdjYzMwMWUwNmE5Y2Y0ZTg2ZjgyODIxNDRiYTA5IiwiaWF0IjoxNTU2NDkwNDE
yLCJleHAiOjAsIm5iciI6MTU1NjQ5MDQxMn0.KQhlN5bdiEPVB_m85VV3CVIA
_Ux5CI24AHoer6iElAbGLLPrwvN0ntHsagUFyrhk6edvDofRvG6Z1o5F4NS8Cg]]></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

storage/passwords

`https://<host>:<mPort>/services/storage/passwords`
Create or update user credentials, or list credentials for all users.

Authorization

The `list_storage_passwords` capability is required for the GET operation. The `edit_storage_passwords` capability is required for the POST operation.

Usage details

The password credential is the only part of the user credentials that is stored securely. It is encrypted with a secure key resident on the same server.

GET

List available credentials.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
clear_password	Clear text password.
encr_password	Encrypted, stored password.
password	Password mask, always ********.
realm	Realm in which credentials are valid.
username	User name associated with credentials.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/storage/passwords
```

XML Response

```
.
.
.
<title>passwords</title>
 <id>https://localhost:8089/services/storage/passwords</id>
 <updated>2014-06-30T13:43:06-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/storage/passwords/_new" rel="create"/>
 <link href="/services/storage/passwords/_reload" rel="_reload"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>:testuser:</title>
   <id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A</id>
   <updated>2014-06-30T13:43:06-07:00</updated>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="alternate"/>
   <author>
     <name>admin</name>
   </author>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="list"/>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="edit"/>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="clear_password">newpwd</s:key>
       <s:key name="eai:acl">
         <s:dict>
```

```
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="encr_password">$1$prTUy3vRWg==</s:key>
      <s:key name="password">********</s:key>
      <s:key name="realm"></s:key>
      <s:key name="username">testuser</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Create/update new credentials.

Request parameters

Name	Type	Description
name	String	**Required**. Credentials username.
password	String	**Required**. Credentials user password.
realm	String	Credentials realm.

Response keys

Name	Description
encr_password	Encrypted, stored password.
password	Password mask, always `********`.
realm	Realm in which credentials are valid.

Name	Description
username	Username associated with credentials.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/passwords -d name=user1 -d
password=changeme2
```

XML Response

```
.
.
.
<title>passwords</title>
 <id>https://localhost:8089/services/storage/passwords</id>
 <updated>2014-06-30T13:51:44-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/storage/passwords/_new" rel="create"/>
 <link href="/services/storage/passwords/_reload" rel="_reload"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>:user1:</title>
   <id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Auser1%3A</id>
   <updated>2014-06-30T13:51:44-07:00</updated>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="alternate"/>
   <author>
     <name>admin</name>
   </author>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="list"/>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="edit"/>
   <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="clear_password">changeme2</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">search</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">admin</s:key>
           <s:key name="perms">
```

```
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="encr_password">$1$q7nC1WvQY/pGcQ==</s:key>
      <s:key name="password">********</s:key>
      <s:key name="realm"></s:key>
      <s:key name="username">user1</s:key>
    </s:dict>
  </content>
</entry>
```

storage/passwords/{name}

`https://<host>:<mPort>/services/storage/passwords/<name>`

Update, delete, or list credentials for the `{name}` user.

Authorization

The `edit_storage_passwords` capability is required for the DELETE and POST operations. The `list_storage_passwords` capability is required for the GET operation.

DELETE

Delete the specified user credentials.

Usage details

The `{name}` portion of the URL must be bounded by the colon (:) symbol as in this example.

```
/services/storage/passwords/:uname:
```

Request parameters

None

Response keys

Returns a list of the remaining credentials in the {name} namespace.

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE
https://localhost:8089/servicesNS/nobody/search/storage/passwords/:user1:
```

XML Response

```
 <title>passwords</title>
 <id>https://localhost:8089/services/storage/passwords</id>
 <updated>2014-06-30T14:21:11-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/storage/passwords/_new" rel="create"/>
 <link href="/services/storage/passwords/_reload" rel="_reload"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

GET

Access the specified user credentials.

Request parameters

None

Response keys

Name	Description
clear_password	Clear text password.
encr_password	Encrypted, stored password.
password	Password mask, always `********`.
realm	Realm in which credentials are valid.
username	User name associated with credentials.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/passwords/user1
```

XML Response

```
 <title>passwords</title>
 <id>https://localhost:8089/services/storage/passwords</id>
 <updated>2014-06-30T14:06:04-07:00</updated>
```

```
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/storage/passwords/_new" rel="create"/>
<link href="/services/storage/passwords/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>:user1:</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Auser1%3A</id>
  <updated>2014-06-30T14:06:04-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="clear_password">changeme2</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list/>
          </s:key>
          <s:key name="requiredFields">
            <s:list>
```

```
               <s:item>password</s:item>
             </s:list>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="encr_password">$1$q7nC1WvQY/pGcQ==</s:key>
       <s:key name="password">********</s:key>
       <s:key name="realm"></s:key>
       <s:key name="username">user1</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Update the specified user credentials.

Request parameters

Name	Type	Description
password	String	User password credential.

Response keys

Name	Description
clear_password	Clear text password.
encr_password	Encrypted, stored password.
password	Password mask, always `********`.
realm	Realm in which credentials are valid.
username	User name associated with credentials.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/passwords/splunker -d
password=changemeAgain
```

XML Response

```
.
.
.
<title>passwords</title>
 <id>https://localhost:8089/services/storage/passwords</id>
 <updated>2014-06-30T14:13:57-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
```

```
</author>
<link href="/services/storage/passwords/_new" rel="create"/>
<link href="/services/storage/passwords/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>:user1:</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Auser1%3A</id>
  <updated>2014-06-30T14:13:57-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="clear_password">changemeAgain</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="encr_password">$1$q7nC1WvQY/p0UtMdIVM=</s:key>
      <s:key name="password">********</s:key>
      <s:key name="realm"></s:key>
      <s:key name="username">user1</s:key>
    </s:dict>
  </content>
</entry>
```

Application endpoints

Application endpoint descriptions

Manage applications.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud limitations

If you have a managed Splunk Cloud deployment with search head clustering and index clustering, the REST API supports access to the search head only. You can use the REST API to interact with the search head in your deployment. Using the REST API to access any other cluster member nodes is not supported. For example, application endpoints are not applicable to Splunk Cloud deployments.

---

apps/appinstall (deprecated)

`https://<host>:<port>/services/apps/appinstall`

Install or update an application.

> This endpoint is deprecated as of software version 6.6.0. To create an app or see a list of apps, see apps/local in this topic.

POST

Install or update an application from a local file or URL.

Request parameters

Name	Type	Description
name	String	**Required**. Full Unix or Windows path of the `.tgz` or `.spl` app source file. The path can be on the local disk or a URL.
update	Boolean	Indicates whether to update installed app. `true` = update existing app, overwriting the existing app folder. `false` = [Default] install new app.

Response keys

Response might be delayed while app installs.

Name	Description
location	Installed location `$SPLUNK_HOME/etc/apps/<app_name>`.
name	App name.
source_location	App source file location, the path *name* request parameter.
status	Install status. `installed` = Successfully installed.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/appinstall/ -d
name=c:/tmp/splunk-dashboard-examples_50.tgz
```

XML Response

```
.
.
.
 <title></title>
 <id>https://localhost:8089/services/apps/appinstall</id>
 <updated>2014-07-01T09:44:41-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/appinstall/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>dashboard_examples</title>
   <id>https://localhost:8089/services/apps/appinstall/dashboard_examples</id>
   <updated>2014-07-01T09:44:41-07:00</updated>
   <link href="/services/apps/appinstall/dashboard_examples" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/apps/appinstall/dashboard_examples" rel="list"/>
   <content type="text/xml">
```

```
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="location">C:\Program Files\Splunk\etc\apps\dashboard_examples</s:key>
      <s:key name="name">dashboard_examples</s:key>
      <s:key name="source_location">c:/tmp/splunk-dashboard-examples_50.tgz</s:key>
      <s:key name="status">installed</s:key>
    </s:dict>
  </content>
</entry>
```

apps/apptemplates

`https://<host>:<port>/services/apps/apptemplates`

List installed app templates. You can use an app template as the *template* parameter in a POST to `/services/apps/local`.

For additional information, see apps/local.

GET

List installed app templates.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

None

Each `<entry>` element includes a `<link>` reference to an app template. The `barebones` and `sample_app` templates are installed by default.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/apptemplates
```

XML Response

```
.
.
.
<title></title>
 <id>https://localhost:8089/services/apps/apptemplates</id>
 <updated>2014-07-01T09:50:36-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>2</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>barebones</title>
   <id>https://localhost:8089/services/apps/apptemplates/barebones</id>
   <updated>2014-07-01T09:50:36-07:00</updated>
   <link href="/services/apps/apptemplates/barebones" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/apps/apptemplates/barebones" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
```

```
                <s:item>*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="lol">wut</s:key>
  </s:dict>
 </content>
</entry>
<entry>
 <title>sample_app</title>
 <id>https://localhost:8089/services/apps/apptemplates/sample_app</id>
 <updated>2014-07-01T09:50:36-07:00</updated>
 <link href="/services/apps/apptemplates/sample_app" rel="alternate"/>
 <author>
   <name>system</name>
 </author>
 <link href="/services/apps/apptemplates/sample_app" rel="list"/>
 <content type="text/xml">
   <s:dict>
     <s:key name="eai:acl">
       <s:dict>
         <s:key name="app"></s:key>
         <s:key name="can_list">1</s:key>
         <s:key name="can_write">1</s:key>
         <s:key name="modifiable">0</s:key>
         <s:key name="owner">system</s:key>
         <s:key name="perms">
           <s:dict>
             <s:key name="read">
               <s:list>
                 <s:item>admin</s:item>
                 <s:item>splunk-system-role</s:item>
               </s:list>
             </s:key>
             <s:key name="write">
               <s:list>
                 <s:item>*</s:item>
               </s:list>
             </s:key>
           </s:dict>
         </s:key>
         <s:key name="removable">0</s:key>
         <s:key name="sharing">system</s:key>
       </s:dict>
     </s:key>
     <s:key name="lol">wut</s:key>
   </s:dict>
 </content>
</entry>
```

apps/apptemplates/{name}

```
https://<host>:<port>/services/apps/apptemplates/{name}
```

Get the `{name}` app template descriptor.

For additional information, see apps/apptemplates.

GET

Get the `{name}` app template descriptor.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/apptemplates/sample_app
```

XML Response

```
.
.
.
 <title></title>
 <id>https://localhost:8089/services/apps/apptemplates</id>
 <updated>2014-07-01T09:54:23-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>sample_app</title>
   <id>https://localhost:8089/services/apps/apptemplates/sample_app</id>
   <updated>2014-07-01T09:54:23-07:00</updated>
   <link href="/services/apps/apptemplates/sample_app" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/apps/apptemplates/sample_app" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
```

```
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list/>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="lol">wut</s:key>
    </s:dict>
  </content>
</entry>
```

apps/local

```
https://<host>:<port>/services/apps/local
```

Create an app or list installed apps and properties.

> The capabilities that this endpoint requires change based on the enable_install_apps setting in limits.conf. If this setting is true, the install_apps and edit_local_apps settings are required. If this setting is false, the admin_all_objects capability is required. By default, this setting value is false but you can change it on your system to improve security.

GET

List installed apps and properties.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
author	App author and optional contact information. For apps deployed on Splunkbase, the Splunkbase account username.
check_for_updates	Indicates whether to check for updates. `true` = Check Splunkbase for app updates. `false` = Do not check Splunkbase for app updates.
configured	Custom setup complete indication: `true` = Custom app setup complete. `false` = Custom app setup not complete.
description	App description.
details	URL to use for detailed information about the app.
disabled	App state indication. `true` = App is disabled. `false` = App is enabled.
label	App name.
state_change_requires_restart	Indicates whether to require restart on state change. `true` = App state change requires restart. `false` = App state change might not require restart depending on other restart requirements.
version	App version.
visible	Indicates whether app is visible and navigable from Splunk Web. `true` = App is visible and navigable. `false` = App is not visible and navigable.

Application usage

Splunkbase can correlate locally-installed apps with the same app on Splunkbase for update notifications.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local
```

XML Response

```
<title>localapps</title>
  <id>https://localhost:17001/services/apps/local</id>
  <updated>2015-10-13T17:53:03-07:00</updated>
  <generator build="a1c9b18fdcfc" version="6.3.0"/>
  <author>
  <name>Splunk</name>
  </author>
  <link href="/services/apps/local/_new" rel="create"/>
  <link href="/services/apps/local/_reload" rel="_reload"/>
  <link href="/services/apps/local/_acl" rel="_acl"/>
  <opensearch:totalResults>16</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>alert_logevent</title>
    <id>https://localhost:17001/servicesNS/nobody/system/apps/local/alert_logevent</id>
    <updated>2015-10-13T17:53:03-07:00</updated>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent" rel="list"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent" rel="edit"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent" rel="remove"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent/disable" rel="disable"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_logevent/package" rel="package"/>
<content type="text/xml">
      <s:dict>
        <s:key name="author">Splunk</s:key>
        <s:key name="check_for_updates">1</s:key>
        <s:key name="configured">1</s:key>
        <s:key name="core">1</s:key>
        <s:key name="description">Log Event Alert Action</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
           <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="label">Log Event Alert Action</s:key>
        <s:key name="managed_by_deployment_client">0</s:key>
        <s:key name="show_in_nav">1</s:key>
        <s:key name="state_change_requires_restart">0</s:key>
        <s:key name="version">6.4.0</s:key>
        <s:key name="visible">0</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
```

```
    <title>alert_webhook</title>
    <id>https://localhost:17001/servicesNS/nobody/system/apps/local/alert_webhook</id>
<updated>2015-10-13T17:53:03-07:00</updated>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook" rel="list"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook" rel="edit"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook" rel="remove"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook/disable" rel="disable"/>
    <link href="/servicesNS/nobody/system/apps/local/alert_webhook/package" rel="package"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="author">Splunk</s:key>
        <s:key name="check_for_updates">1</s:key>
        <s:key name="configured">1</s:key>
        <s:key name="core">1</s:key>
        <s:key name="description">Webhook Alert Action</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="label">Webhook Alert Action</s:key>
        <s:key name="managed_by_deployment_client">0</s:key>
        <s:key name="show_in_nav">1</s:key>
        <s:key name="state_change_requires_restart">0</s:key>
        <s:key name="version">6.4.0</s:key>
        <s:key name="visible">0</s:key>
      </s:dict>
    </content>
  </entry>
<entry>
    <title>appsbrowser</title>
    <id>https://localhost:17001/servicesNS/nobody/system/apps/local/appsbrowser</id>
```

```
   <updated>2015-10-13T17:53:03-07:00</updated>
   <link href="/servicesNS/nobody/system/apps/local/appsbrowser" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/apps/local/appsbrowser" rel="list"/>
   <link href="/servicesNS/nobody/system/apps/local/appsbrowser/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/apps/local/appsbrowser" rel="edit"/>
   <link href="/servicesNS/nobody/system/apps/local/appsbrowser/package" rel="package"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="author">Splunk</s:key>
       <s:key name="check_for_updates">1</s:key>
       <s:key name="configured">1</s:key>
       <s:key name="core">1</s:key>
       <s:key name="description">Browse apps available to install.</s:key>
       <s:key name="disabled">0</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">system</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">0</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>power</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">app</s:key>
         </s:dict>
       </s:key>
       <s:key name="label">Apps Browser</s:key>
       <s:key name="managed_by_deployment_client">0</s:key>
       <s:key name="show_in_nav">0</s:key>
       <s:key name="state_change_requires_restart">0</s:key>
       <s:key name="version">6.4.0</s:key>
       <s:key name="visible">1</s:key>
     </s:dict>
   </content>
 </entry>
<entry>
   <title>framework</title>
   <id>https://localhost:17001/servicesNS/nobody/system/apps/local/framework</id>
   <updated>2015-10-13T17:53:03-07:00</updated>
   <link href="/servicesNS/nobody/system/apps/local/framework" rel="alternate"/>
   <author>
```

```
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/apps/local/framework" rel="list"/>
  <link href="/servicesNS/nobody/system/apps/local/framework/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/apps/local/framework" rel="edit"/>
  <link href="/servicesNS/nobody/system/apps/local/framework" rel="remove"/>
  <link href="/servicesNS/nobody/system/apps/local/framework/disable" rel="disable"/>
  <link href="/servicesNS/nobody/system/apps/local/framework/package" rel="package"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="check_for_updates">1</s:key>
      <s:key name="configured">0</s:key>
      <s:key name="core">1</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="label">framework</s:key>
      <s:key name="managed_by_deployment_client">0</s:key>
      <s:key name="show_in_nav">1</s:key>
      <s:key name="state_change_requires_restart">0</s:key>
      <s:key name="visible">0</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>gettingstarted</title>
  <id>https://localhost:17001/servicesNS/nobody/system/apps/local/gettingstarted</id>
  <updated>2015-10-13T17:53:03-07:00</updated>
  <link href="/servicesNS/nobody/system/apps/local/gettingstarted" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/apps/local/gettingstarted" rel="list"/>
  <link href="/servicesNS/nobody/system/apps/local/gettingstarted/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/apps/local/gettingstarted" rel="edit"/>
```

```
    <link href="/servicesNS/nobody/system/apps/local/gettingstarted" rel="remove"/>
    <link href="/servicesNS/nobody/system/apps/local/gettingstarted/enable" rel="enable"/>
    <link href="/servicesNS/nobody/system/apps/local/gettingstarted/package" rel="package"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="author">Splunk</s:key>
        <s:key name="check_for_updates">1</s:key>
        <s:key name="configured">1</s:key>
        <s:key name="core">1</s:key>
        <s:key name="description">Get started with Splunk.  This app introduces you to many of Splunk's
features.  You'll learn how to use Splunk to index data, search and investigate, add knowledge, monitor and
alert, report and analyze.</s:key>
        <s:key name="disabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>power</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="label">Getting started</s:key>
        <s:key name="managed_by_deployment_client">0</s:key>
        <s:key name="show_in_nav">1</s:key>
        <s:key name="state_change_requires_restart">0</s:key>
        <s:key name="version">1.0</s:key>
        <s:key name="visible">1</s:key>
      </s:dict>
    </content>
  </entry>
.
.
.
```

POST

Create an app.

Usage details

- Splunkbase can correlate locally installed apps with the same app on Splunkbase for update notifications.
- The app folder name cannot include spaces or special characters.

Request parameters

Name	Type	Description
auth	String	Splunkbase session token for operations like install and update that require login. Use *auth* or *session* when installing or updating an app through Splunkbase.
author	String	For apps posted to Splunkbase, use your Splunk account username. For internal apps, include your name and contact information.
configured	Boolean	Custom setup complete indication: `true` = Custom app setup complete. `false` = Custom app setup not complete.
description	String	Short app description also displayed below the app title in Splunk Web Launcher.
explicit_appname	String	Custom app name. Overrides *name* when installing an app from a file where *filename* is set to `true`. See also *filename*.
filename	Boolean	Indicates whether to use the *name* value as the app source location. `true` indicates that *name* is a path to a file to install. `false` indicates that *name* is the literal app name and that the app is created from Splunkbase using a template.
label	String	App name displayed in Splunk Web, from five to eighty characters excluding the prefix "Splunk for".
name	String	**Required**. Literal app name or path for the file to install, depending on the value of *filename*. *filename* = `false` indicates that *name* is the literal app name and that the app is created from Splunkbase using a template. *filename* = `true` indicates that *name* is the URL or path to the local `.tar`, `.tgz` or `.spl` file. If *name* is the Splunkbase URL, set *auth* or *session* to authenticate the request. The app folder name cannot include spaces or special characters.
session	String	Login session token for installing or updating an app on Splunkbase. Alternatively, use *auth*.
template	Enum	App template to use when creating the app" `barebones` - [Default] Basic app framework. `sample_app` - Example views and searches. Any custom app template.
update	Boolean	File-based update indication: `true` specifies that *filename* should be used to update an existing app. If not specified, *update* defaults to `false`, which indicates that *filename* should not be used to update an existing app.
version	String	App version.
visible	Boolean	Indicates whether the app is visible and navigable from Splunk Web. `true` = App is visible and navigable. `false` = App is not visible or navigable.

Response keys

Name	Description
author	

Name	Description
	For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.
check_for_updates	`true` = Check Splunkbase for app updates. `false` = Do not check Splunkbase for app updates.
configured	Custom setup completeness indication. `true` = Custom app setup complete. `false` = Custom app setup not complete.
description	Brief app description, displayed below the app title in Splunk Web.
disabled	App state indication. `true` = App is disabled. `false` = App is enabled.
label	App name displayed in Splunk Web.
name	Installed app name, which might differ from the POST *name* parameter.
state_change_requires_restart	Indicates whether restart required on state change. `true` = App state change requires restart. `false` = App state change might not require restart, depending on other restart requirements.
version	App version.
visible	Indicates whether app is visible and navigable from Splunk Web. `true` = App is visible and navigable. `false` = App is not visible or navigable.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local -d name=restDemo
```

XML Response

```
<title></title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2014-07-01T10:09:37-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>restDemo</title>
   <id>https://localhost:8089/servicesNS/nobody/system/apps/local/restDemo</id>
   <updated>2014-07-01T10:09:37-07:00</updated>
   <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="list"/>
   <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="edit"/>
   <link href="/servicesNS/nobody/system/apps/local/restDemo/package" rel="package"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="author"></s:key>
       <s:key name="check_for_updates">1</s:key>
       <s:key name="configured">0</s:key>
       <s:key name="description"></s:key>
       <s:key name="disabled">0</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">system</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">0</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>power</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">app</s:key>
         </s:dict>
       </s:key>
       <s:key name="label">restDemo</s:key>
       <s:key name="name">restDemo</s:key>
       <s:key name="state_change_requires_restart">0</s:key>
       <s:key name="version">1.0</s:key>
       <s:key name="visible">1</s:key>
     </s:dict>
   </content>
 </entry>
```

apps/local/{name}

`https://<host>:<port>/services/apps/local/{name}`

Manage `{name}` app. For additional information, see "Uninstall an app" in the *Admin Manual*.

DELETE

Delete the `{name}` app.

Usage details

- Use the /apps/local GET method to confirm that the app is no longer installed.
- See "Uninstall an app" for additional manual cleanup that might be needed after deleting an app.

Request parameters

None

Response keys

A message is displayed that might indicate a restart is required.

Specifying the name of a non-existent app returns an error message, as shown below.

```
In handler 'localapps': Could not find object id=<app_name>.
```

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/apps/local/sample_app
```

XML Response

```
.
.
.
 <title>localapps</title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2014-07-15T10:24:35-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 <link href="/services/apps/local/_reload" rel="_reload"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages>
   <s:msg type="INFO">Restart required by: indexes</s:msg>
 </s:messages>
```

GET

List information about the `{name}` app.

Request parameters

Name	Type	Description
refresh	Boolean	Indicates whether to reload any objects associated with the `{name}` app indication: `true` = Reload objects. `false` = Do not reload objects.

Response keys

Name	Description
author	For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.
check_for_updates	Indicates whether to check for updates. `true` = Check Splunkbase for app updates. `false` = Do not check Splunkbase for app updates.
configured	Custom setup completeness indication. `true` = Custom app setup complete. `false` = Custom app setup not complete.
description	Brief app description also displayed below the app title in Splunk Web.
disabled	App state indication: `true` = App is disabled. `false` = App is enabled.
label	App name displayed in Splunk Web, from five to 80 characters and excluding the prefix "Splunk For".
state_change_requires_restart	Indicates whether restart is required on state change indication: `true` = App state change requires restart. `false` = App state change might not require restart, depending on other restart requirements.
version	App version.
visible	App is visible and navigable from Splunk Web indication: `true` = App is visible and navigable. `false` = App is not visible or navigable.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/dashboard_examples
```

XML Response

```
.
.
.
<title>localapps</title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2014-07-01T10:23:46-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 <link href="/services/apps/local/_reload" rel="_reload"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>dashboard_examples</title>
   <id>https://localhost:8089/servicesNS/nobody/system/apps/local/dashboard_examples</id>
   <updated>2014-07-01T10:23:46-07:00</updated>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples" rel="list"/>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples" rel="edit"/>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples" rel="remove"/>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples/disable" rel="disable"/>
   <link href="/servicesNS/nobody/system/apps/local/dashboard_examples/package" rel="package"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="author">Splunk, Inc.</s:key>
       <s:key name="check_for_updates">1</s:key>
       <s:key name="configured">0</s:key>
       <s:key name="description"><![CDATA[Example dashboards, forms, and views for Splunk 5+. This is the
succesor app to UI Examples 4.1+. Splunk Dashboard Examples contains over 50 examples updated for Splunk 5.
Each example contains inline documenation to help get you started building Splunk dashboards.]]></s:key>
       <s:key name="details">https://splunkbase.splunk.com/apps/id/dashboard_examples</s:key>
       <s:key name="disabled">0</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">system</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">0</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">app</s:key>
         </s:dict>
       </s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list>
               <s:item>author</s:item>
               <s:item>check_for_updates</s:item>
```

```
              <s:item>configured</s:item>
              <s:item>description</s:item>
              <s:item>label</s:item>
              <s:item>version</s:item>
              <s:item>visible</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="label">Splunk Dashboard Examples</s:key>
      <s:key name="state_change_requires_restart">0</s:key>
      <s:key name="version">5.0</s:key>
      <s:key name="visible">1</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update the `{name}` app properties. Append `/enable` or `/disable` to enable or disable the app. See Enable and disable endpoint for more information.

Request parameters

Name	Type	Description
author	String	For apps posted to Splunkbase, use your Splunk account username. For internal apps, use your full name and contact information.
check_for_updates	Boolean	Check for updates indicator. `true` = Check Splunkbase for app updates. `false` = Do not check Splunkbase for app updates.
configured	Boolean	Custom setup completion indicator. `true` = Custom app setup complete. `false` = Custom app setup not complete.
description	String	Short app description also displayed below the app title in Splunk Web.
label	String	App name displayed in Splunk Web, from five to 80 characters and excluding the prefix "Splunk For".
version	String	App version.
visible	Boolean	Indicates whether app is visible and navigable from Splunk Web. `true` = App is visible and navigable. `false` = App is not visible and navigable.

Response keys

Name	Description
author	For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.

Name	Description
check_for_updates	Check for updates indication: `true` = Check Splunkbase for app updates. `false` = Do not check Splunkbase for app updates.
configured	Custom setup completion indicator. `true` = Custom app setup complete. `false` = Custom app setup not complete.
description	App description also displayed below the app title in Splunk Web.
disabled	App state indication. `true` = App is disabled. `false` = App is enabled.
label	App name displayed in Splunk Web, from five to 80 characters and excluding the prefix "Splunk For".
state_change_requires_restart	Restart required on state change indication: `true` = App state change requires restart. `false` = App state change might not require restart, depending on other restart requirements.
version	App version.
visible	Indicator of whether app is visible and navigable from Splunk Web. `true` = App is visible and navigable. `false` = App is not visible or navigable.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/restDemo -d version=1.1
```

XML Response

```
.
.
.
<title>localapps</title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2014-07-01T10:28:35-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 <link href="/services/apps/local/_reload" rel="_reload"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>restDemo</title>
   <id>https://localhost:8089/servicesNS/nobody/system/apps/local/restDemo</id>
   <updated>2014-07-01T10:28:35-07:00</updated>
   <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
```

```
  <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="list"/>
  <link href="/servicesNS/nobody/system/apps/local/restDemo/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="edit"/>
  <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="remove"/>
  <link href="/servicesNS/nobody/system/apps/local/restDemo/package" rel="package"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="author"></s:key>
      <s:key name="check_for_updates">1</s:key>
      <s:key name="configured">0</s:key>
      <s:key name="description"></s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="label">restDemo</s:key>
      <s:key name="state_change_requires_restart">0</s:key>
      <s:key name="version">1.1</s:key>
      <s:key name="visible">1</s:key>
    </s:dict>
  </content>
</entry>
```

apps/local/{name}/package

The packaging action is deprecated.

`https://<host>:<port>/services/apps/local/{name}/package`

Archive the `{name}` app as a `.spl` file in the `$SPLUNK_HOME/etc/system/static/app-packages` directory.

GET

Archive the `{name}.spl` app.

Usage details

Download the archived app using the following URL:

```
https://host:<port>/static/app-packages/{name}.spl
```

Request parameters

None

Response keys

Name	Description
name	App name and name of the folder containing the app.
path	Local path to an archive of the app.
url	App download URL.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/restDemo/package
```

XML Response

```
.
.
.
 <title></title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2014-07-01T10:46:43-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>Package</title>
   <id>https://localhost:8089/services/apps/local/Package</id>
   <updated>2014-07-01T10:46:43-07:00</updated>
   <link href="/services/apps/local/Package" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/apps/local/Package/setup" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="name">restDemo</s:key>
       <s:key name="path">C:\Program Files\Splunk\etc\system\static\app-packages\restDemo.spl</s:key>
       <s:key name="url">https://localhost:8089/static/app-packages/restDemo.spl</s:key>
     </s:dict>
   </content>
 </entry>
```

apps/local/{name}/setup

`https://<host>:<port>/services/apps/local/{name}/setup`
Get the `{name}` app setup information.

GET

Get setup information for the `{name}` app.

Usage details

Some apps contain setup scripts that must be run before the app is enabled. For those apps, the `setup.xml` file must exist in the `$SPLUNK_BASE\etc\apps\<appname>\default` directory.

Request parameters

None

Response keys

Name	Description
<script location>	TBD
eai:setup	CDATA setup script location.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/unix/setup
```

XML Response

```
.
.
.
 <title>localapps</title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2011-07-13T11:24:35-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>unix</title>
   <id>https://localhost:8089/servicesNS/nobody/unix/apps/local/unix</id>
   <updated>2011-07-13T11:24:35-07:00</updated>
   <link href="/servicesNS/nobody/unix/apps/local/unix" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/unix/apps/local/unix/setup" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="/admin/script/.%252Fbin%252Fcpu.sh/enabled">1</s:key>
       <s:key name="/admin/script/.%252Fbin%252Fcpu.sh/interval">30</s:key>
       <s:key name="/admin/script/.%252Fbin%252Fdf.sh/enabled">1</s:key>
       <s:key name="/admin/script/.%252Fbin%252Fdf.sh/interval">300</s:key>
       ... elided ...
       <s:key name="/admin/script/.%252Fbin%252Fwho.sh/enabled">1</s:key>
       <s:key name="/admin/script/.%252Fbin%252Fwho.sh/interval">150</s:key>
       ... eai:acl element elided ...
       ... eai:attributes element elided ...
       <s:key name="eai:setup">
<![CDATA[<?xml version="1.0" encoding="UTF-8"?> <SetupInfo> <block title="Welcome to the Splunk for nix
App"> <text>The Splunk for nix app provides some sample searches and reports to boot-strap your use of
Splunk for Unix host management. To work, it needs certain inputs enabled. These system metrics drive the
sample dashboards. Please review and confirm the inputs below before proceeding.</text> </block> <block
title="CPU Stats (sar / mpstat / etc.)" endpoint="admin/script" entity=".%252Fbin%252Fcpu.sh"> <input
field="interval" id="/admin/script/.%252Fbin%252Fcpu.sh/interval"> <label>Polling Interval (sec)</label>
<type>text</type> </input> <input field="enabled" id="/admin/script/.%252Fbin%252Fcpu.sh/enabled">
<label>Enable</label> <type>bool</type> </input> </block>

. . .
<block title="Time Query (date, ntpdate -q)" endpoint="admin/script" entity=".%252Fbin%252Ftime.sh"> <input
field="interval" id="/admin/script/.%252Fbin%252Ftime.sh/interval"> <label>Polling Interval (sec)</label>
<type>text</type> </input> <input field="enabled" id="/admin/script/.%252Fbin%252Ftime.sh/enabled">
<label>Enable</label> <type>bool</type> </input> </block> <block title="Linux Audit Log
(/var/log/audit/audit.log | ausearch)" endpoint="admin/script" entity=".%252Fbin%252Frlog.sh"> <input
field="interval" id="/admin/script/.%252Fbin%252Frlog.sh/interval"> <label>Polling Interval (sec)</label>
<type>text</type> </input> <input field="enabled" id="/admin/script/.%252Fbin%252Frlog.sh/enabled">
<label>Enable</label> <type>bool</type> </input> </block> <block title="Warning"> <text>Submitting this form
can take a long time. Please be patient and wait for it to complete before navigating away from this
page.</text> </block> </SetupInfo> ]]> </s:key>

     </s:dict>
   </content>
 </entry>
```

apps/local/{name}/update

```
https://<host>:<port>/services/apps/local/{name}/update
```

Get `eai:acl` information for the `{name}` app.

GET

Get `{name}` app `eai:acl` information.

Request parameters
None

Response keys
The *eai:acl* key of the `{name}` app.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/gettingstarted/update
```

XML Response

```
.
.
.
 <title>localapps</title>
 <id>https://localhost:8089/services/apps/local</id>
 <updated>2014-07-15T10:34:13-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/apps/local/_new" rel="create"/>
 <link href="/services/apps/local/_reload" rel="_reload"/>
```

```
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>gettingstarted</title>
  <id>https://localhost:8089/services/apps/local/gettingstarted</id>
  <updated>2014-07-15T10:34:13-07:00</updated>
  <link href="/services/apps/local/gettingstarted" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/apps/local/gettingstarted" rel="list"/>
  <link href="/services/apps/local/gettingstarted/_reload" rel="_reload"/>
  <link href="/services/apps/local/gettingstarted" rel="edit"/>
  <link href="/services/apps/local/gettingstarted" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

Cluster endpoints

Cluster endpoint descriptions

Manage indexer clusters and search head clusters in Splunk Enterprise.

To distinguish indexer cluster endpoints from search cluster endpoints, note:

- Indexer cluster endpoints: Endpoints that contain `cluster` in their URIs pertain to indexer clusters.
- Search head cluster endpoints: Endpoints that contain `shcluster` in their URIs pertain to search head clusters.

> The values manager and peer replace the prior values of master and slave. The prior values are currently still supported, but they will be removed from the product in a future release.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. Cluster endpoints are generally not accessible in Splunk Cloud Platform.

Authorized users can access and configure other indexer cluster nodes, including indexer or cluster manager, or license manager nodes, in the Splunk Cloud Platform manager user interface.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

Indexer cluster endpoints

The endpoints in this section pertain to **indexer clusters**.

All endpoints that contain `cluster` in their URIs pertain to indexer clusters. In this section, if a URI contains the term **search head**, it refers to search head nodes in the indexer cluster. The term **peer node** refers to peer nodes in the indexer cluster. For more information about indexer cluster architecture, see The basics of indexer cluster architecture and Search head configuration overview in the *Managing Indexers and Clusters of Indexers* manual.

cluster/config

`https://<host>:<mPort>/services/cluster/config`

Access cluster node configuration details.

GET

List cluster node configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
cxn_timeout	Low-level timeout, in seconds, for establishing connection between cluster nodes. Defaults to 60 seconds.
disabled	Indicates if this node is disabled.
forwarderdata_rcv_port	The port from which to receive data from a forwarder.
forwarderdata_use_ssl	Indicates whether to use SSL when receiving data from a forwarder.
heartbeat_period	Only valid for peer nodes in a cluster. The time, in seconds, that a peer attempts to send a heartbeat to the manager
heartbeat_timeout	Only valid for the manager node in a cluster configuration. The time, in seconds, before a manager considers a peer down. Once a peer is down, the manager initiates steps to replicate buckets from the dead peer to its live peers. Defaults to 60 seconds.
manager_uri	Valid only for nodes configured as a peer or searchhead. URI of the cluster manager to which this node connects.
max_peer_build_load	The number of jobs that a peer can have in progress at any time that make the bucket searchable.
max_peer_rep_load	Maximum number of replications that can be ongoing as a target.
mode	Valid values: (manager | peer | searchhead | disabled) Defaults to disabled. Sets operational mode for this cluster node. Only one manager may exist per cluster.
ping_flag	For internal use to facilitate communication between the manager and peers.

Name	Description
quiet_period	The time, in seconds, that a manager waits for peers to add themselves to the cluster.
rcv_timeout	Low-level timeout, in seconds, for receiving data between cluster nodes. Defaults to 60 seconds.
register_forwarder_address	Not used. Reserved for future use.
register_replication_address	Valid only for nodes configured as peers. The address on which a peer is available for accepting replication data. This is useful in the cases where a peer host machine has multiple interfaces and only one of them can be reached by another splunkd instance.
register_search_address	IP address that advertises this indexer to search heads.
rep_cxn_timeout	Low-level timeout, in seconds, for establishing a connection for replicating data.
rep_max_rcv_timeout	Maximum cumulative time, in seconds, for receiving acknowledgement data from peers. Defaults to 600s.
rep_max_send_timeout	Maximum time, in seconds, for sending replication slice data between cluster nodes. Defaults to 600s.
rep_rcv_timeout	Low-level timeout, in seconds, for receiving data between cluster nodes.
rep_send_timeout	Low-level timeout, in seconds, for sending replication data between cluster nodes. Defaults to 5 seconds.
replication_factor	Only valid for nodes configured as a manager. Determines how many copies of raw data are created in the cluster. This could be less than the number of cluster peers. Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.
replication_port	TCP port to listen for replicated data from another cluster member.
replication_use_ssl	Indicates whether to use SSL when sending replication data.
restart_timeout	Only valid for nodes configured as a manager. The amount of time, in seconds, the manager waits for a peer to come back when the peer is restarted (to avoid the overhead of trying to fix the buckets that were on the peer). Defaults to 600 seconds. *Note:* This only works if the peer is restarted from Splunk Web.
search_factor	Only valid for nodes configured as a manager. Determines how many searchable copies of each bucket to maintain. Must be less than or equal to replication_factor and greater than 0. Defaults to 2.
secret	Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the manager, it is not able to communicate with the manager. Corresponds to pass4SymmKey setting in `server.conf`.
send_timeout	Low-level timeout, in seconds, for sending data between cluster nodes. Defaults to 60 seconds.
summary_replication	Boolean indicator of whether summary replication is on or off. A `true` value means that it is turned on.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/config
```

XML Response

```
<title>clusterconfig</title>
 <id>https://localhost:8089/services/cluster/config</id>
 <updated>2012-09-05T10:19:49-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/config/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>config</title>
   <id>https://localhost:8089/services/cluster/config/config</id>
   <updated>2012-09-05T10:19:49-07:00</updated>
   <link href="/services/cluster/config/config" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/config/config" rel="list"/>
   <link href="/services/cluster/config/config/_reload" rel="_reload"/>
   <link href="/services/cluster/config/config" rel="edit"/>
   <link href="/services/cluster/config/config/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="cxn_timeout">60</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl node elided ...
       <s:key name="forwarderdata_rcv_port">0</s:key>
       <s:key name="forwarderdata_use_ssl">1</s:key>
       <s:key name="heartbeat_period">1</s:key>
       <s:key name="heartbeat_timeout">60</s:key>
       <s:key name="manager_uri"></s:key>
       <s:key name="max_peer_build_load">5</s:key>
       <s:key name="max_peer_rep_load">5</s:key>
       <s:key name="mode">manager</s:key>
       <s:key name="ping_flag">1</s:key>
       <s:key name="quiet_period">60</s:key>
       <s:key name="rcv_timeout">60</s:key>
       <s:key name="register_forwarder_address"></s:key>
       <s:key name="register_replication_address"></s:key>
       <s:key name="register_search_address"></s:key>
       <s:key name="rep_cxn_timeout">5</s:key>
       <s:key name="rep_max_rcv_timeout">600</s:key>
       <s:key name="rep_max_send_timeout">600</s:key>
       <s:key name="rep_rcv_timeout">10</s:key>
       <s:key name="rep_send_timeout">5</s:key>
       <s:key name="replication_factor">2</s:key>
       <s:key name="replication_port"></s:key>
       <s:key name="replication_use_ssl">0</s:key>
       <s:key name="restart_timeout">600</s:key>
       <s:key name="search_factor">2</s:key>
       <s:key name="secret">********</s:key>
       <s:key name="send_timeout">60</s:key>
     </s:dict>
   </content>
 </entry>
```

cluster/config/config

`https://<host>:<mPort>/services/cluster/config/config`

Manage cluster node configuration details.

GET

List cluster node configuration.

This operation works identically to the GET on `cluster/config`.

POST

Manage configuration details.

See Indexer cluster configuration overview in *Managing Indexers and Clusters of Indexers* and the `[clustering]` stanza options in the server.conf spec file for more details on indexer cluster configuration.

Request parameters

Name	Datatype	Description
available_sites	N/A	Sets the various sites that are recognized for this manager. Valid values include `site1` to `site64`.
cluster_label	String	Label for this cluster.
cxn_timeout	Number	Low-level timeout, in seconds, for establishing connection between cluster nodes. Defaults to 60 seconds.
heartbeat_period	Number	Only valid for peer nodes in a cluster. Time, in seconds, that a peer attempts to send a heartbeat to the manager
heartbeat_timeout	Number	Only valid for the manager node in a cluster configuration. Time, in seconds, before a manager considers a peer down. Once a peer is down, the manager initiates steps to replicate buckets from the dead peer to its live peers. Defaults to 60 seconds.
manager_uri	URI	Valid only for nodes configured as a peer or searchhead. URI of the cluster manager to which this node connects.
max_peer_build_load	Number	The number of jobs that a peer can have in progress at any time that make the bucket searchable.
max_peer_rep_load	Number	Maximum number of replications that can be ongoing as a target.
mode	See description.	Required. Valid values: (manager | peer | searchhead | disabled) Defaults to disabled. Sets operational mode for this cluster node. Only one manager may exist per cluster.
multisite	Boolean	Enable or disable the multisite feature for this cluster.
notify_scan_period	Non-zero number	Controls the frequency that the indexer scans summary folders for summary updates. Only used when `summary_replication` is enabled on the manager. Defaults to 10 seconds.

Name	Datatype	Description
ping_flag	N/A	For internal use to facilitate communication between the manager and peers.
quiet_period	Number	The time, in seconds, that a manager waits for peers to add themselves to the cluster.
rcv_timeout	Number	Low-level timeout, in seconds, for receiving data between cluster nodes. Defaults to 60 seconds.
register_forwarder_address	N/A	Reserved for future use.
register_replication_address	See description.	Valid only for nodes configured as peers. The address on which a peer is available for accepting replication data. This is useful in the cases where a peer host machine has multiple interfaces and only one of them can be reached by another splunkd instance.
register_search_address	N/A	IP address that advertises this indexer to search heads.
rep_cxn_timeout	Number	Low-level timeout, in seconds, for establishing a connection for replicating data.
rep_max_rcv_timeout	Number	Maximum cumulative time, in seconds, for receiving acknowledgement data from peers. Defaults to 600s.
rep_max_send_timeout	Number	Maximum time, in seconds, for sending replication slice data between cluster nodes. Defaults to 600s.
rep_rcv_timeout	Number	Low-level timeout, in seconds, for receiving data between cluster nodes.
rep_send_timeout	Number	Low-level timeout, in seconds, for sending replication data between cluster nodes. Defaults to 5 seconds.
replication_factor	Number	Only valid for nodes configured as a manager. Determines how many copies of raw data are created in the cluster. This could be less than the number of cluster peers. Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.
replication_port	Number	TCP port to listen for replicated data from another cluster member.
replication_use_ssl	Number	Indicates whether to use SSL when sending replication data.
restart_timeout	Number	Only valid for nodes configured as a manager. The amount of time, in seconds, the manager waits for a peer to come back when the peer is restarted (to avoid the overhead of trying to fix the buckets that were on the peer). Defaults to 600 seconds. *Note:* This only works if the peer is restarted from Splunk Web.
search_factor	Number	Only valid for nodes configured as a manager. Determines how many searchable copies of each bucket to maintain. Must be less than or equal to replication_factor and greater than 0. Defaults to 2.
secret	N/A	Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the manager, it is not able to communicate with the manager. Corresponds to pass4SymmKey setting in `server.conf`.
send_timeout	Number	Low-level timeout, in seconds, for sending data between cluster nodes. Defaults to 60 seconds.
site	N/A	Site ID for peer/searchhead indexer. Valid values include `site1` to `site64`.
site_replication_factor	Number	Replication factor for a multisite configuration.
site_search_factor	Number	Search factor for a multisite configuration.
summary_replication	Boolean	Enable or disable summary replication.
use_batch_mask_changes	Boolean	Only valid for `mode=manager` .Specifies if the manager should process bucket mask changes in batch or inidividually one by one. Defaults to true. Set to false when there are 6.1 peers in the cluster for backwards compatibility.

Name	Datatype	Description

Response data keys

None.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/config/config -d cxn_timeout=59
```

XML Response

```
  <title>clusterconfig</title>
  <id>https://localhost:8089/services/cluster/config</id>
  <updated>2015-12-07T17:09:48-08:00</updated>
  <generator build="917abedc8bb44ec1c225a6eb730808a606174cf0" version="20151123"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/config/_reload" rel="_reload"/>
  <link href="/services/cluster/config/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/buckets

```
https://<host>:<mPort>/services/cluster/manager/buckets
```

Provides bucket configuration information for a cluster manager node.

GET

List cluster manager node bucket configuration.

Request parameters

Use an `&summaries=true` field in the query string to show summaries.

Use one or more filters in the query string to select buckets or bucket states. For example, use this URL to filter buckets returned for both the `main` index and `StreamingSource` status.

```
https://localhost:8089/services/cluster/manager /buckets?filter=index=main&filter=status=StreamingSource
```

See the following table for available filters.

Filter name	Datatype	Description
index	String	Index name.
status	String	Bucket state. Available options are • StreamingSource • StreamingTarget • Complete • StreamingError • PendingTruncate Bucket is scheduled to truncate. • PendingDiscard Bucket is scheduled to discard. • NonStreamingTarget
search_state	String	Bucket search state. Available options are • Searchable • Unsearchable • PendingSearchable Bucket scheduled to become searchable by transferring or building tsidx files. • PendingUnsearchable Bucket is scheduled to become unsearchable. • SearchablePendingMask Primary change is scheduled or in progress.
replication_count	Number	Use <, >, != or = with numbers to indicate filtering values.
search_count	Number	Use <, >, != or = with numbers to indicate filtering values.
bucket_size	Number	Use <, >, != or = with numbers to indicate filtering values.
frozen	Boolean true | false	Return frozen buckets or non-frozen buckets.
has_primary	Boolean true | false	Return buckets with primaries or without primaries.
meets_multisite_replication_count	Boolean true | false	Return buckets that meet cluster replication policy or buckets that do not meet cluster replication policy.
meets_multisite_search_count	Boolean true | false	Return buckets that meet cluster search policy or buckets that do not meet cluster search policy.
multisite_bucket	Boolean true | false	Return buckets created in multisite mode or buckets not created in multisite mode.
origin_site	String	Site of the indexer where buckets were created.
standalone	Boolean true | false	Use true or 1 to return standalone buckets. Use false or 0 to return clustered buckets.

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
bucket_size	Indicates the size, in bytes, of the bucket.
constrain_to_origin_site	Flag indicating this particular bucket is a clustered pre-multisite bucket. Such buckets are replicated only within their origin site.
frozen	Indicates if the bucket is frozen.
index	Name of the index to which the bucket belongs.
origin_site	Where the bucket originated.

Name	Description
peers	Lists information about buckets on peers to this manager.
primaries_by_site	Primary peer (GIUD).
rep_count_by_site	Number of buckets.
search_count_by_site	Number of searchable buckets.
service_after_time	Bucket service is deferred until after this time.
standalone	Indicates if the bucket was created on the peer before the peer entered into a cluster configuration with this manager.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/buckets
```

XML Response

```
<title>clustermanagerbuckets</title>
 <id>https://localhost:8089/services/cluster/manager/buckets</id>
 <updated>2014-04-17T19:13:57+00:00</updated>
 <generator build="204899" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/manager/buckets/_new" rel="create"/>
 <opensearch:totalResults>24</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEEAB</title>
   <id>https://localhost:8089/services/cluster/manager/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEEAB<
/id>
   <updated>2014-04-17T19:13:57+00:00</updated>
   <link href="/services/cluster/manager/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEEAB"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEEAB" rel="list"/>
   <link href="/services/cluster/manager/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEEAB"
rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="bucket_size">47187</s:key>
       <s:key name="constrain_to_origin_site">1</s:key>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="frozen">0</s:key>
       <s:key name="index">_audit</s:key>
       <s:key name="origin_site">site2</s:key>
       <s:key name="peers">
```

```
        <s:dict>
          <s:key name="238C3311-F0A4-4A9B-97F0-53667CFFEEAB">
            <s:dict>
              <s:key name="bucket_flags">0x6</s:key>
              <s:key name="checksum"></s:key>
              <s:key name="checksum_state">StableCksum</s:key>
              <s:key name="search_state">Searchable</s:key>
              <s:key name="status">Complete</s:key>
            </s:dict>
          </s:key>
          <s:key name="C878FADC-513D-4BDD-BA48-F25BB82FE565">
            <s:dict>
              <s:key name="bucket_flags">0x0</s:key>
              <s:key name="checksum"></s:key>
              <s:key name="checksum_state">StableCksum</s:key>
              <s:key name="search_state">Searchable</s:key>
              <s:key name="status">Complete</s:key>
            </s:dict>
          </s:key>
          <s:key name="E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C">
            <s:dict>
              <s:key name="bucket_flags">0x0</s:key>
              <s:key name="checksum"></s:key>
              <s:key name="checksum_state">StableCksum</s:key>
              <s:key name="search_state">Unsearchable</s:key>
              <s:key name="status">Complete</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="primaries_by_site">
        <s:dict>
          <s:key name="site1">238C3311-F0A4-4A9B-97F0-53667CFFEEAB</s:key>
          <s:key name="site2">238C3311-F0A4-4A9B-97F0-53667CFFEEAB</s:key>
        </s:dict>
      </s:key>
      <s:key name="rep_count_by_site">
        <s:dict>
          <s:key name="site2">3</s:key>
        </s:dict>
      </s:key>
      <s:key name="search_count_by_site">
        <s:dict>
          <s:key name="site2">2</s:key>
        </s:dict>
      </s:key>
      <s:key name="service_after_time">0</s:key>
      <s:key name="standalone">0</s:key>
    </s:dict>
  </content>
</entry>
<entry>
    .
    .
    .
  elided
    .
    .
    .
<entry>
  <title>_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</title>
  <id>https://localhost:8089/services/cluster/manager/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7
```

```
-C3A4BB6B518C</id>
   <updated>2014-04-17T19:13:57+00:00</updated>
   <link href="/services/cluster/manager/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C"
rel="list"/>
   <link href="/services/cluster/manager/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C"
rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="bucket_size"></s:key>
       <s:key name="constrain_to_origin_site">0</s:key>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="frozen">0</s:key>
       <s:key name="index">_internal</s:key>
       <s:key name="origin_site">site2</s:key>
       <s:key name="peers">
         <s:dict>
           <s:key name="61666763-43E9-411B-9464-D80A5119EF0E">
             <s:dict>
               <s:key name="bucket_flags">0x2</s:key>
               <s:key name="checksum"></s:key>
               <s:key name="checksum_state">StableCksum</s:key>
               <s:key name="search_state">Searchable</s:key>
               <s:key name="status">StreamingTarget</s:key>
             </s:dict>
           </s:key>
           <s:key name="C878FADC-513D-4BDD-BA48-F25BB82FE565">
             <s:dict>
               <s:key name="bucket_flags">0x0</s:key>
               <s:key name="checksum"></s:key>
               <s:key name="checksum_state">StableCksum</s:key>
               <s:key name="search_state">Unsearchable</s:key>
               <s:key name="status">StreamingTarget</s:key>
             </s:dict>
           </s:key>
           <s:key name="E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C">
             <s:dict>
               <s:key name="bucket_flags">0x4</s:key>
               <s:key name="checksum"></s:key>
               <s:key name="checksum_state">StableCksum</s:key>
               <s:key name="search_state">Searchable</s:key>
               <s:key name="status">StreamingSource</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="primaries_by_site">
         <s:dict>
           <s:key name="site1">61666763-43E9-411B-9464-D80A5119EF0E</s:key>
           <s:key name="site2">E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</s:key>
         </s:dict>
       </s:key>
       <s:key name="rep_count_by_site">
         <s:dict>
           <s:key name="site1">1</s:key>
           <s:key name="site2">2</s:key>
```

```
    </s:dict>
   </s:key>
   <s:key name="search_count_by_site">
    <s:dict>
     <s:key name="site1">1</s:key>
     <s:key name="site2">1</s:key>
    </s:dict>
   </s:key>
   <s:key name="service_after_time">0</s:key>
   <s:key name="standalone">0</s:key>
  </s:dict>
 </content>
</entry>
```

cluster/manager/buckets/{name}

`https://<host>:<mPort>/services/cluster/manager/buckets/{name}`

Access bucket configuration information.

GET

List bucket configuration information.

Request parameters

The `filter` parameter of the Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
bucket_size	Indicates the size, in bytes, of the bucket.
constrain_to_origin_site	Flag indicating this particular bucket is a clustered pre-multisite bucket. Such buckets are replicated only within their origin site.
frozen	Indicates if the bucket is frozen.
index	Name of the index to which the bucket belongs.
origin_site	Where the bucket originated.
peers	Lists information about buckets on peers to this manager.
primaries_by_site	Primary peer (GIUD).
rep_count_by_site	Number of buckets.
search_count_by_site	Number of searchable buckets.
service_after_time	Bucket service is deferred until after this time.
standalone	Indicates if the bucket was created on the peer before the peer entered into a cluster configuration with this manager.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/cluster/manager/buckets/internal~1~238C3311-F0A4-4A9B-97F0-53667CFFEEAB
```

XML Response

```
<title>clustermanagerbuckets</title>
 <id>https://localhost:8089/services/cluster/manager/buckets</id>
 <updated>2014-04-17T19:16:03+00:00</updated>
 <generator build="204899" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/manager/buckets/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>_internal~1~238C3311-F0A4-4A9B-97F0-53667CFFEEAB</title>
   <id>https://localhost:8089/services/cluster/manager/buckets/_internal~1~238C3311-F0A4-4A9B-97F0
-53667CFFEEAB</id>
   <updated>2014-04-17T19:16:03+00:00</updated>
   <link href="/services/cluster/manager/buckets/_internal~1~238C3311-F0A4-4A9B-97F0-53667CFFEEAB"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/buckets/_internal~1~238C3311-F0A4-4A9B-97F0-53667CFFEEAB"
rel="list"/>
   <link href="/services/cluster/manager/buckets/_internal~1~238C3311-F0A4-4A9B-97F0-53667CFFEEAB"
rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="bucket_size"></s:key>
       <s:key name="constrain_to_origin_site">0</s:key>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="eai:attributes">
         ... elided ...
       </s:key>
       <s:key name="frozen">0</s:key>
       <s:key name="index">_internal</s:key>
       <s:key name="origin_site">site2</s:key>
       <s:key name="peers">
         <s:dict>
           <s:key name="238C3311-F0A4-4A9B-97F0-53667CFFEEAB">
             <s:dict>
               <s:key name="bucket_flags">0x4</s:key>
               <s:key name="checksum"></s:key>
               <s:key name="checksum_state">StableCksum</s:key>
               <s:key name="search_state">Searchable</s:key>
               <s:key name="status">StreamingSource</s:key>
             </s:dict>
           </s:key>
```

```
          <s:key name="29F9560E-A44A-425C-8753-1C6158B46C84">
            <s:dict>
              <s:key name="bucket_flags">0x2</s:key>
              <s:key name="checksum"></s:key>
              <s:key name="checksum_state">StableCksum</s:key>
              <s:key name="search_state">Searchable</s:key>
              <s:key name="status">StreamingTarget</s:key>
            </s:dict>
          </s:key>
          <s:key name="C878FADC-513D-4BDD-BA48-F25BB82FE565">
            <s:dict>
              <s:key name="bucket_flags">0x0</s:key>
              <s:key name="checksum"></s:key>
              <s:key name="checksum_state">StableCksum</s:key>
              <s:key name="search_state">Unsearchable</s:key>
              <s:key name="status">StreamingTarget</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="primaries_by_site">
        <s:dict>
          <s:key name="site1">29F9560E-A44A-425C-8753-1C6158B46C84</s:key>
          <s:key name="site2">238C3311-F0A4-4A9B-97F0-53667CFFEEAB</s:key>
        </s:dict>
      </s:key>
      <s:key name="rep_count_by_site">
        <s:dict>
          <s:key name="site1">1</s:key>
          <s:key name="site2">2</s:key>
        </s:dict>
      </s:key>
      <s:key name="search_count_by_site">
        <s:dict>
          <s:key name="site1">1</s:key>
          <s:key name="site2">1</s:key>
        </s:dict>
      </s:key>
      <s:key name="service_after_time">0</s:key>
      <s:key name="standalone">0</s:key>
    </s:dict>
  </content>
</entry>
```

cluster/manager/buckets/{bucket_id}/fix

`https://<host>:<mPort>/services/cluster/manager/buckets/{bucket_id}/fix`
Add the specified bucket to the fix list.

For more information, see Bucket-fixing scenarios in *Managing Indexers and Clusters of Indexers*.

Authentication and Authorization
Requires the `admin` role or `indexes_edit` capability.

POST

Add this bucket to the fix list.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/services/cluster/manager/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/fix
-X POST
```

XML Response

```
  <title>clustermanagerbuckets</title>
  <id>https://localhost:8089/services/cluster/manager/buckets</id>
  <updated>2015-11-04T12:23:57-08:00</updated>
  <generator build="8effae892620f7b651853d141b7b7a6b61b929c0" version="20151102"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/buckets/_new" rel="create"/>
  <link href="/services/cluster/manager/buckets/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/buckets/{bucket_id}/fix_corrupt_bucket

`https://<host>:<mPort>/services/cluster/manager/buckets/{bucket_id}/fix_corrupt_bucket`

Trigger a corruption fixup of a clustered non-SmartStore-enabled bucket.

For more information, see Bucket-fixing scenarios in *Managing Indexers and Clusters of Indexers*.

Authentication and Authorization

Requires the `admin` role or `edit_indexer_cluster` capability.

POST

Trigger a corruption fixup for this bucket.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/services/cluster/manager/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/fix
_corrupt_bucket -X POST
```

XML Response

```
  "links":{
      "create":"/services/cluster/manager/buckets/_new"
   },
   "origin":"https://chieftain:15511/services/cluster/manager/buckets",
   "updated":"2023-09-06T22:30:08-07:00",
   "generator":{
      "build":"479782058d4faa7ef3404e947f4117df3a59654c",
      "version":"20230905"
   },
   "entry":[

   ],
   "paging":{
      "total":0,
      "perPage":30,
      "offset":0
   },
   "messages":[

   ]
```

cluster/manager/buckets/{bucket_id}/freeze

`https://<host>:<mPort>/services/cluster/manager/buckets/{bucket_id}/freeze`

Set the bucket's state to frozen. The frozen state may not persist after a cluster manager restart unless one of the peers has set the frozen state. A POST to this endpoint does not set the bucket's state to frozen on peers.

> **Note:** Use this endpoint with caution. It is recommended to test the endpoint in a test cluster prior to use on an actual bucket.

For more information, see How the cluster handles frozen buckets in *Managing Indexers and Clusters of Indexers*.

Authentication and Authorization

Requires the `admin` role or `indexes_edit` capability.

POST

Set this bucket's state to frozen.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/cluster/manager/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/freeze
-X POST
```

XML Response

```
  <title>clustermanagerbuckets</title>
  <id>https://locahost:8089/services/cluster/manager/buckets</id>
  <updated>2015-11-04T12:21:27-08:00</updated>
  <generator build="8effae892620f7b651853d141b7b7a6b61b929c0" version="20151102"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/buckets/_new" rel="create"/>
  <link href="/services/cluster/manager/buckets/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/buckets/{bucket_id}/remove_all

`https://<host>:<mPort>/services/cluster/manager/buckets/{bucket_id}/remove_all`
Delete all copies of the specified bucket.

> **Caution:** Using this endpoint will cause irreversible data loss. It is recommended to test the endpoint on a test cluster prior to use on an actual bucket.

Authentication and Authorization
Requires the `admin` role or `indexes_edit` capability.

POST

Delete all copies of the specified bucket.

Request parameters

None

Returned values

None. If an invalid bucket id is used, an error message is returned.

```
<response>
  <messages>
    <msg type="ERROR">
 In handler 'clustermanagerbuckets': bucket not found</msg>
  </messages>
</response>
```

If the request is made on a hot bucket, an error message is returned.

```
<response>
  <messages>
    <msg type="ERROR">
 In handler 'clustermanagerbuckets': cannot remove hot bucket from cluster</msg>
  </messages>
</response>
```

Example request and response

XML Request

```
curl -k -u admin:password
https://localhost:8089/services/cluster/manager/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/remove_all
-X POST
```

XML Response

```
<title>clustermanagerbuckets</title>
  <id>https://localhost:8089/services/cluster/manager/buckets</id>
  <updated>2015-11-04T12:24:12-08:00</updated>
  <generator build="8effae892620f7b653d141b7b7a6b61b929c0" version="20151102"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/buckets/_new" rel="create"/>
  <link href="/services/cluster/manager/buckets/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/buckets/{bucket_id}/remove_from_peer

`https://<host>:<mPort>/services/cluster/manager/buckets/{bucket_id}/remove_from_peer`

Deletes the copy of this bucket from specified peer.

If the request causes the cluster to lose its complete state, the cluster will engage in fixup activities. This may result in another copy of the same bucket appearing on this peer. If, however, the specified bucket is frozen, the cluster does not attempt any fixup activities.

> **Caution:** Using this endpoint will cause irreversible data loss. It is recommended to test the endpoint on a test-cluster prior to use on an actual bucket.

Authentication and Authorization

Requires the `admin` role or `indexes_edit` capability.

POST

Delete this bucket from specified peer. Set bucket state to frozen

Request parameters

Name	Type	Description
peer (required)	GUID	Peer GUID

Returned values

None. If the `peer` parameter is missing from the request, an error message is returned.

```
<response>
  <messages>
    <msg type="ERROR">
 In handler 'clustermanagerbuckets': The following required arguments are missing: peer.</msg>
  </messages>
</response>
```

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/cluster/manager/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/remove
_from_peer -X POST -d peer=222275BA-00DF-4CFE-9AEC-48A87B97EC71
```

XML Response

```
 <title>clustermanagerbuckets</title>
  <id>https://localhost:8089/services/cluster/manager/buckets</id>
  <updated>2015-11-04T12:23:18-08:00</updated>
  <generator build="8effae892620f7b651853d141b7b7a6b61b929c0" version="20151102"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/buckets/_new" rel="create"/>
  <link href="/services/cluster/manager/buckets/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/control/control/prune_index

```
https://<host>:<mPort>/services/cluster/manager/control/control/prune_index
```

Clean up excess bucket copies across an index.

For more information, see Remove extra bucket copies in *Managing Indexers and Clusters of Indexers*.

POST

Clean up excess bucket copies across an index.

Request parameters

Name	Description
index	Optional. The index from which to remove excess bucket copies. If not specified, the POST operation clears excess bucket copies across all indexes.

Returned values

None

Example request

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/control/control/prune_index -d
index="my_index"
```

cluster/manager/control/control/rebalance_primaries

```
https://<host>:<mPort>/services/cluster/manager/control/control/rebalance_primaries
```

Rebalance primary bucket copies across peers. For more information, see Rebalance the indexer cluster primary buckets in *Managing Indexers and Clusters of Indexers*.

POST

Rebalance primary buckets across all peers of this manager.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/control/control/rebalance_primaries
--request POST
```

XML Response

```
<title>clustermanagercontrol</title>
 <id>https://localhost:8089/services/cluster/manager/control</id>
 <updated>2013-08-21T13:08:52-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

cluster/manager/control/control/remove_peers

```
https://<host>:<mPort>/services/cluster/manager/control/control/remove_peers
```

Remove one or more peers.

See also

cluster/manager/peers

POST

Remove one or more peers.

Request parameters

Name	Type	Description
peers **Required**	String	One or more comma-separated peer GUIDs.

Returned values
None

Application usage

If peer `status` is not `Down` or `GracefulShutdown`, the interface returns the following error message:

```
<response>
  <messages>
    <msg type="ERROR">
 In handler 'clustermanagercontrol': Remove aborted, Reason: Peer=<hostname> with guid=<peerID> cannot be
removed. Peer has status=Up. Only peers with status=Down (or) GracefulShutdown can be removed.</msg>
  </messages>
</response>
```

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/control/control/remove_peers --request
POST  -d "peers=F2AA19BD-622F-4F8C-A8E0-1233"
```

XML Response

```
 <title>clustermanagercontrol</title>
 <id>https://localhost:8089/services/cluster/manager/control</id>
 <updated>2014-09-10T13:12:54-07:00</updated>
 <generator build="230688" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
```

cluster/manager/control/control/resync_bucket_from_peer

`https://<host>:<mPort>/services/cluster/manager/control/control/resync_bucket_from_peer`
This endpoint resets the state of a specified bucket based on the current state of the bucket at a peer.

POST

Reset bucket state based on the current state of the bucket at a peer.

Request Parameters

Name	Type	Default	Description
bucket_id	String	N/A	**Required**. ID of bucket to update.
peer	GUID	N/A	**Required**. GUID of peer from which to update the bucket.

Returned Values
None.

Example request and response

XML Request

```
curl -k -u admin:pass
https://hostname:mPort:/services/cluster/manager/control/control/resync_bucket_from_peer -X POST -d
bucket_id=_audit~2~8F6747E9-88C9-4488-8806-4EA3CA433CF5 -d peer=8F6747E9-88C9-4488-8806-4EA3CA433CF5
```

XML Response

```
  <title>clustermanagercontrol</title>
  <id>https://10.66.129.225:8089/services/cluster/manager/control</id>
  <updated>2016-06-30T14:32:06+08:00</updated>
  <generator build="9904f7fc29b" version="6.4.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/control/control/roll-hot-buckets

```
https://<host>:<mPort>/services/cluster/manager/control/control/roll-hot-buckets
```

This endpoint forces a specified bucket in an indexer cluster to roll from hot to warm. Pass the bucket id (bid) to the manager node. The manager instructs the origin peer for that bucket to roll its copy. In turn, the origin peer tells all the replicating peers to roll their copies

You might discover a bucket that is stuck in fixup and needs to be rolled using logs, Splunk Web, or either of the following two endpoints.

- cluster/manager/fixup
- cluster/manager/buckets

Authorization and authentication
This endpoint requires the admin role for use.

POST

Force a bucket to roll from hot to warm.

Request parameters

Name	Type	Default	Description
bucket_id	String	N/A	**Required**. ID for bucket to roll.

Returned values

None.

Example request and response

XML Request

```
curl -k -u username:password
https://localhost:8089/services/cluster/manager/control/control/roll-hot-buckets -X POST -d
"bucket_id=_audit~2~1A3889D7-954B-4CE6-B071-01B438DE9865"
```

XML Response

```
<title>clustermanagercontrol</title>
  <id>https://localhost:8089/services/cluster/manager/control</id>
  <updated>2015-10-30T07:34:56+08:00</updated>
  <generator build="0d98363e4338" version="6.4.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/control/control/rolling_upgrade_finalize

```
https://<host>:<mPort>/services/cluster/manager/control/control/rolling_upgrade_finalize
```

Finalizes an indexer cluster rolling upgrade.

POST

Finalizes an indexer cluster rolling upgrade.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/cluster/manager/control/control/rolling_upgrade_finalize -X POST
```

XML Response

```
<title>clustermanagercontrol</title>
  <id>https://10.141.65.179:52000/services/cluster/manager/control</id>
  <updated>2018-04-01T22:04:46+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Cluster is no longer in searchable rolling upgrade mode.</s:msg>
  </s:messages>
```

cluster/manager/control/control/rolling_upgrade_init

`https://<host>:<mPort>/services/cluster/manager/control/control/rolling_upgrade_init`
Initializes an indexer cluster rolling upgrade.

POST

Initializes an indexer cluster rolling upgrade.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/control/control/rolling_upgrade_init
-X POST
```

XML Response

```
  <title>clustermanagercontrol</title>
  <id>https://10.141.65.179:52000/services/cluster/manager/control</id>
  <updated>2018-04-01T21:06:21+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Cluster is now in searchable rolling upgrade mode.</s:msg>
  </s:messages>
```

cluster/manager/control/default/abort_restart

`https://<host>:<mPort>/services/cluster/manager/control/default/abort_restart`

Aborts an ongoing restart of an indexer cluster.

Authentication and Authorization

Requires the `admin` role or `edit_indexer_cluster` capability.

POST

Abort an ongoing restart of an indexer cluster.

Request parameters

None

Returned values

None

Example request and response

JSON Request

```
curl -k -u admin:password -X POST
"https://chieftain:15511/services/cluster/manager/control/default/abort_restart?output_mode=json"
```

JSON Response

```
  {
   "links":{

   },
   "origin":"https://chieftain:15511/services/cluster/manager/control",
   "updated":"2023-09-06T23:45:53-07:00",
   "generator":{
      "build":"479782058d4faa7ef3404e947f4117df3a59654c",
      "version":"20230905"
   },
   "entry":[

   ],
   "paging":{
      "total":0,
      "perPage":30,
      "offset":0
   },
   "messages":[
      {
         "type":"INFO",
         "text":"Aborting the rolling restart initiated successfully. List of peers skipped restarting:
E30CA8C0-23E5-4A6B-9F28-D2EC991CCD75,9E3FED8B-59A0-4B95-8116-F8F8A67A7686,32790C7F-82CB-4E39-8689
-3600F72D4D01,2B6C57ED-9FFC-44F0-9E58-CD8BE3519F3F,5A65CEB6-79A6-40D7-914C-4859DEACF79B,8C2DC775-EB8E-44D7-AFF8
-38482B3A9990,033085C7-F31B-467D-9577-B8A5E5131810"
      }
   ]
}
```

cluster/manager/control/default/apply

`https://<host>:<mPort>/services/cluster/manager/control/default/apply`

Pushes a bundle.

POST

Push a bundle.

Request Parameters

Name	Type	Default	Description
skip-validation	Boolean	False	Set as true to skip the validation step for this bundle.
ignore_identical_bundle	Boolean	True	Set as false to push this bundle even if current active bundle is identical to this bundle.

Returned Values

None.

Example request and response

XML Request

```
curl -k -u admin:pass https://host:mPort/services/cluster/manager/control/default/apply -X POST
```

XML Response

```
<title>clustermanagercontrol</title>
<id>https://wimpy:7420/services/cluster/manager/control</id>
<updated>2019-01-02T13:46:04-08:00</updated>
<generator build="c5340c4d9387ab182815dc279bcd14979b747dc9" version="20181119"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/cluster/manager/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>clusterbundles</title>
<id>https://wimpy:7420/services/cluster/manager/control/clusterbundles</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/cluster/manager/control/clusterbundles" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/cluster/manager/control/clusterbundles" rel="list"/>
<link href="/services/cluster/manager/control/clusterbundles" rel="edit"/>
<content type="text/xml">
<s:dict>
<s:key name="checksum">288845778D5B1952F534AB16DD82881E</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
</s:dict>
</content>
</entry>
</feed>
```

cluster/manager/control/default/cancel_bundle_push

`https://<host>:<mPort>/services/cluster/manager/control/default/cancel_bundle_push`

Cancels and resets the bundle push operation. Use this endpoint when the cluster manager does not receive a validation response from the cluster peer due to an error. For more information, see Configuration bundle issues.

POST

Cancel and reset the bundle push operation.

Request Parameters

None.

Returned Values

None.

Example request and response

XML Request

```
curl -k -u admin:pass https://host:mPort/services/cluster/manager/control/default/cancel_bundle_push -X POST
```

XML Response

```
  <title>clustermanagercontrol</title>
  <id>https:/<hostname>:<mgt-port>/services/cluster/manager/control</id>
  <updated>2017-08-21T15:13:13-07:00</updated>
  <generator build="3d1811a2a4dda9f4751be7cc71833cc377f62da8" version="20170823"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/manager/control/default/maintenance

`https://<host>:<mPort>/services/cluster/manager/control/default/maintenance`

Put the cluster manager into maintenance mode.

POST

Toggle maintenance mode.

Request Parameters

Name	Datatype	Description
mode	Boolean	Enable or disable maintenance mode on the cluster manager.

Returned Values

None.

Example request and response

XML Request

```
curl -k -u username:pass https://<host>:<mPort>/services/cluster/manager/control/default/maintenance -d
mode=true
```

XML Response

```
<title>clustermanagercontrol</title>
<id>https://myserver:8089/services/cluster/manager/control</id>
<updated>2020-05-15T05:45:49+00:00</updated>
<generator build="a6754d8441bf" version="8.0.3"/>
<author>
<name>Splunk</name>
</author>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>
```

cluster/manager/control/default/rollback

`https://<host>:<mPort>/services/cluster/manager/control/default/rollback`

Roll a bundle back to the previously active bundle.

POST

Roll back a bundle.

Request Parameters

None.

Returned Values

None.

Example request and response

XML Request

```
curl -k -u admin:pass https://host:mPort/services/cluster/manager/control/default/rollback -X POST
```

XML Response

```
<title>clustermanagercontrol</title>
<id>https://wimpy:7420/services/cluster/manager/control</id>
<updated>2019-01-02T13:46:26-08:00</updated>
<generator build="c5340c4d9387ab182815dc279bcd14979b747dc9" version="20181119"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/cluster/manager/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>clusterbundles</title>
<id>https://wimpy:7420/services/cluster/manager/control/clusterbundles</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/cluster/manager/control/clusterbundles" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/cluster/manager/control/clusterbundles" rel="list"/>
<link href="/services/cluster/manager/control/clusterbundles" rel="edit"/>
<content type="text/xml">
<s:dict>
<s:key name="checksum">447F196DB0CF55389029A950E3C2D3E3</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
</s:dict>
</content>
</entry>
</feed>
```

cluster/manager/control/default/validate_bundle

`https://<host>:<mPort>/services/cluster/manager/control/default/validate_bundle`

Tests if the bundle in `etc/manager-apps` passes validation. Optionally, tests if the bundle will trigger an indexer restart.

POST

Validate a bundle.

Request Parameters

Name	Type	Default	Description
check-restart	Boolean	False	By default, checks if the bundle passes validation on the cluster manager and indexers. Set to true to check if the bundle will trigger a restart on the indexers.

Returned Values

None.

Example request and response

XML Request

```
curl -k -u admin:pass https://host:mPort/services/cluster/manager/control/default/validate_bundle -d
check-restart=true -X POST
```

XML Response

```
<title>clustermanagercontrol</title>
<id>https://wimpy:7420/services/cluster/manager/control</id>
<updated>2019-01-02T13:56:48-08:00</updated>
<generator build="c5340c4d9387ab182815dc279bcd14979b747dc9" version="20181119"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/cluster/manager/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>clusterbundles</title>
<id>https://wimpy:7420/services/cluster/manager/control/clusterbundles</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/cluster/manager/control/clusterbundles" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/cluster/manager/control/clusterbundles" rel="list"/>
<link href="/services/cluster/manager/control/clusterbundles" rel="edit"/>
<content type="text/xml">
<s:dict>
```

```
<s:key name="checksum">288845778D5B1952F534AB16DD82881E</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
</s:dict>
</content>
</entry>
</feed>
```

cluster/manager/fixup

`https://<host>:<mPort>/services/cluster/manager/fixup`

Access a list of buckets on a specific fixup priority level. Bucket fixups are processed in order of priority level. See *Request parameters* below for priority level details.

When you access a particular fixup level, buckets may appear in it even though they do not need fixup at this level. Initially, each bucket requiring fixup is added to all levels, even though it might only require processing in a subset of all levels. As the bucket is processed through a level, it is deleted from that level.

GET

List buckets on the specified fixup level.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Datatype	Description

Name	Datatype	Description
level	String	**Required**. Fixup priority level. Use one of the following level values, listed in order of priority. • `corruption` : Corrupted buckets. • `streaming` : Hot buckets that need to be rolled or have their size committed. • `data_safety` : Buckets without at least two `rawdata` copies. • `generation` : Buckets without a primary copy. • `replication_factor` : Buckets without replication factor number of copies. • `search_factor` : Buckets without search factor number of copies. • `checksum_sync` : Level for syncing a bucket's delete files across all peers that have this bucket. Syncing is determined based on the checksum of all of the delete files.
index	String	Optional. Index name.

Returned values

For each bucket in the specified fixup level, the response includes the following details for the `initial` time when the bucket went into the fixup level and the `latest` time that the bucket was checked.

Name	Description
id	Bucket id.
reason	Initial or latest reason for the bucket being on this fixup level.
timestamp	Timestamp for initial bucket addition to fixup list or latest bucket check.

Example request and response

XML Request

```
curl -k -u admin:password https://localhost:8089/services/cluster/manager/fixup?level=replication_factor
```

XML Response

```
<title>clustermanagerfixup</title>
  <id>https://localhost:8089/services/cluster/manager/fixup</id>
  <updated>2015-11-09T17:05:48-08:00</updated>
  <generator build="802b4ea159bb584c629dcdb8ba57c409b1d5b7ab" version="20151030"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/fixup/_acl" rel="_acl"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222</title>
    <id>https://localhost:8089/services/cluster/manager/fixup/_audit~212~22220097-5E3F-4D26-B301
-ECE3C4CD2222</id>
    <updated>2015-11-09T17:05:48-08:00</updated>
    <link href="/services/cluster/manager/fixup/_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/cluster/manager/fixup/_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222"
```

```
rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="index">_audit</s:key>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">add peer=22220097-5E3F-4D26-B301-ECE3C4CD2222 new bucket</s:key>
            <s:key name="timestamp">1447099323</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason">Missing enough suitable candidates to create replicated copy in order to
meet replication policy. Missing={ site2:1 }</s:key>
            <s:key name="timestamp">1447117547</s:key>
          </s:dict>
        </s:key>
        <s:key name="level">replication_factor</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>_internal~12628~111163F8-61F4-4AB3-A1A7-2EDCB10C1111</title>
    <id>https://localhost:8089/services/cluster/manager/fixup/_internal~12628~111163F8-61F4-4AB3-A1A7
-2EDCB10C1111</id>
    <updated>2015-11-09T17:05:48-08:00</updated>
    <link href="/services/cluster/manager/fixup/_internal~12628~111163F8-61F4-4AB3-A1A7-2EDCB10C1111"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/cluster/manager/fixup/_internal~12628~111163F8-61F4-4AB3-A1A7-2EDCB10C1111"
rel="list"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="index">_internal</s:key>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">add peer=111163F8-61F4-4AB3-A1A7-2EDCB10C1111 new bucket</s:key>
            <s:key name="timestamp">1447099323</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason">Missing enough suitable candidates to create replicated copy in order to meet replication policy. Missing={ site1:1 }</s:key>
            <s:key name="timestamp">1447117547</s:key>
          </s:dict>
        </s:key>
        <s:key name="level">replication_factor</s:key>
      </s:dict>
    </content>
  </entry>
```

cluster/manager/generation

`https://<host>:<mPort>/services/cluster/manager/generation`

Access current generation cluster manager information and create a cluster generation.

GET

List peer nodes participating in the current generation for this manager.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
generation_id	The ID for the current generation for this manager.
generation_peers	Lists the peers for this generation of the cluster.
pending_generation_id	The next generation ID used by the manager when committing a new generation. This value is useful for debugging.
pending_last_attempt	The timestamp of the last attempt to commit to the pending generation ID (if ever).
pending_last_reason	The reason why this peer failed to commit to the pending generation. This parameter is EMPTY if no such attempt was made.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/generation
```

XML Response

```
<title>clustermanagergeneration</title>
 <id>https://localhost:8089/services/cluster/manager/generation</id>
 <updated>2012-09-05T10:39:54-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>manager</title>
   <id>https://localhost:8089/services/cluster/manager/generation/manager</id>
   <updated>2012-09-05T10:39:54-07:00</updated>
   <link href="/services/cluster/manager/generation/manager" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/generation/manager" rel="list"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       <s:key name="generation_id">2</s:key>
       <s:key name="generation_peers">
         <s:dict>
           <s:key name="2AF11DD4-1424-4A14-A522-FB9D055E9516">
             <s:dict>
               <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8389</s:key>
```

```
              <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
            </s:dict>
          </s:key>
          <s:key name="50FCDB42-E167-458D-A6A9-E4587E8F16D9">
            <s:dict>
              <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8189</s:key>
              <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="pending_generation_id">3</s:key>
      <s:key name="pending_last_attempt">0</s:key>
      <s:key name="pending_last_reason"></s:key>
    </s:dict>
  </content>
</entry>
```

POST

Create a cluster generation.

Request parameters

Name	Type	Default	Description
name required	String		The URI of the searchhead node of a cluster upon which to create a new generation.
generation_poll_interval	Number		How often, in seconds, the searchhead polls the manager for generation information. Defaults to 60 seconds.
label	String		Server name for the Splunk platform instance specified by the *name* attribute.
mgmt_port	String		The managment port of searchhead node in a cluster upon which you are creating a new generation.
register_search_address	String		The address on which a peer node is available as search head. This is useful in the cases where a host machine has multiple interfaces and only one of them can be reached by another splunkd instance.

Returned values

Name	Description
generation_id	The ID for the current generation for this manager.
generation_peers	Lists the peers for this generation of the cluster.
pending_generation_id	The next generation ID used by the manager when committing a new generation. This value is useful for debugging.
pending_last_attempt	The timestamp of the last attempt to commit to the pending generation ID (if ever).

Name	Description
pending_last_reason	The reason why this peer failed to commit to the pending generation. This parameter is EMPTY if no such attempt was made.
replication_factor_met	Indicates if the replication factor was met for the cluster.
search_factor_met	Indicates if the search factor was met for the cluster.
was_forced	Indicates next generation was forcibly committed.

Example request and response

XML Request

```
curl -k -u admin:pass https://myserver:8089/services/cluster/manager/generation -d name=foo
```

XML Response

```
<title>clustermanagergeneration</title>
 <id>https://myserver:8089/services/cluster/manager/generation</id>
 <updated>2013-10-31T13:58:51-07:00</updated>
 <generator build="184661" version="20131030"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/manager/generation/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>manager</title>
   <id>https://myserver:8089/services/cluster/manager/generation/manager</id>
   <updated>2013-10-31T13:58:51-07:00</updated>
   <link href="/services/cluster/manager/generation/manager" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/generation/manager" rel="list"/>
   <link href="/services/cluster/manager/generation/manager" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       <s:key name="generation_id">5</s:key>
       <s:key name="generation_peers">
         <s:dict>
           <s:key name="11111111-1111-1111-1111-111111111111">
             <s:dict>
               <s:key name="host_port_pair">myserver.splunk.com:6431</s:key>
               <s:key name="peer">PEER1</s:key>
             </s:dict>
           </s:key>
           <s:key name="22222222-2222-2222-2222-222222222222">
             <s:dict>
               <s:key name="host_port_pair">myserver.splunk.com:6432</s:key>
               <s:key name="peer">PEER2</s:key>
             </s:dict>
           </s:key>
           <s:key name="33333333-3333-3333-3333-333333333333">
             <s:dict>
               <s:key name="host_port_pair">myserver.splunk.com:6433</s:key>
               <s:key name="peer">PEER3</s:key>
```

```
            </s:dict>
          </s:key>
          <s:key name="44444444-4444-4444-4444-444444444444">
            <s:dict>
              <s:key name="host_port_pair">myserver.splunk.com:6434</s:key>
              <s:key name="peer">PEER4</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="pending_generation_id">6</s:key>
      <s:key name="pending_last_attempt">0</s:key>
      <s:key name="pending_last_reason"></s:key>
      <s:key name="replication_factor_met">1</s:key>
      <s:key name="search_factor_met">1</s:key>
      <s:key name="was_forced">0</s:key>
    </s:dict>
  </content>
</entry>
```

cluster/manager/generation/{name}

`https://<host>:<mPort>/services/cluster/manager/generation/{name}`

Access information about a peer node participating in the current generation for the specified search head GUID.

GET

List peer node information of the specified search head GUID.

Request parameters

None

Returned values

Name	Description
generation_id	The ID of the current generation for this manager.
generation_peers	Lists the peers for this generation of the cluster.
pending_generation_id	The next generation ID used by the manager when committing a new generation. This value is useful for debugging.
pending_last_attempt	The timestamp of the last attempt to commit to the pending generation ID (if ever).
pending_last_reason	The reason why this peer failed to commit to the pending generation. This parameter is EMPTY if no such attempt was made.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/generation/manager
```

XML Response

```
<title>clustermanagergeneration</title>
 <id>https://localhost:8089/services/cluster/manager/generation</id>
 <updated>2012-09-05T10:45:27-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>manager</title>
   <id>https://localhost:8089/services/cluster/manager/generation/manager</id>
   <updated>2012-09-05T10:45:27-07:00</updated>
   <link href="/services/cluster/manager/generation/manager" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/generation/manager" rel="list"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       ... eai:attributes node elided ...
       <s:key name="generation_id">2</s:key>
       <s:key name="generation_peers">
         <s:dict>
           <s:key name="2AF11DD4-1424-4A14-A522-FB9D055E9516">
             <s:dict>
               <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8389</s:key>
               <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
             </s:dict>
           </s:key>
           <s:key name="50FCDB42-E167-458D-A6A9-E4587E8F16D9">
             <s:dict>
               <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8189</s:key>
               <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="pending_generation_id">3</s:key>
       <s:key name="pending_last_attempt">0</s:key>
       <s:key name="pending_last_reason"></s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Create a new generation for the specified search head GUID.

Request parameters

Name	Type	Description
generation_poll_interval	Number	How often, in seconds, the searchhead polls the manager for generation information. Defaults to 60 seconds.
label	String	Server name for the search head specified by {name}.
mgmt_port	String	The managment port of searchhead node in a cluster upon which you are creating a new generation.
register_search_address	String	The address on which a peer node is available as search head. This is useful when a host machine has multiple interfaces and only one of them can be reached by another `splunkd` instance.

Returned values

Name	Description
generation_id	The ID for the current generation for this manager.
generation_peers	Lists the peers for this generation of the cluster.
pending_generation_id	The next generation ID used by the manager when committing a new generation. This value is useful for debugging.
pending_last_attempt	The timestamp of the last attempt to commit to the pending generation ID (if ever).
pending_last_reason	The reason why this peer failed to commit to the pending generation. This parameter is EMPTY if no such attempt was made.
replication_factor_met	Indicates if the replication factor was met for the cluster.
search_factor_met	Indicates if the search factor was met for the cluster.
was_forced	Indicates next generation was forcibly committed.

Example request and response

XML Request

```
curl -k -u admin:pass https://myserver:8089/services/cluster/manager/generation/foo -X POST -d
generation_poll_interval=62 -d label=PEER2
```

XML Response

```
 <title>clustermanagergeneration</title>
 <id>https://myserver:8089/services/cluster/manager/generation</id>
 <updated>2013-10-31T14:37:20-07:00</updated>
 <generator build="184661" version="20131030"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/manager/generation/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
```

```
  <title>manager</title>
  <id>https://myserver:8089/services/cluster/manager/generation/manager</id>
  <updated>2013-10-31T14:37:20-07:00</updated>
  <link href="/services/cluster/manager/generation/manager" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/generation/manager" rel="list"/>
  <link href="/services/cluster/manager/generation/manager" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      ... eai:acl node elided ...
      <s:key name="generation_id">5</s:key>
      <s:key name="generation_peers">
        <s:dict>
          <s:key name="11111111-1111-1111-1111-111111111111">
            <s:dict>
              <s:key name="host_port_pair">myserver.splunk.com:6431</s:key>
              <s:key name="peer">PEER1</s:key>
            </s:dict>
          </s:key>
          <s:key name="22222222-2222-2222-2222-222222222222">
            <s:dict>
              <s:key name="host_port_pair">myserver.splunk.com:6432</s:key>
              <s:key name="peer">PEER2</s:key>
            </s:dict>
          </s:key>
          <s:key name="33333333-3333-3333-3333-333333333333">
            <s:dict>
              <s:key name="host_port_pair">myserver.splunk.com:6433</s:key>
              <s:key name="peer">PEER3</s:key>
            </s:dict>
          </s:key>
          <s:key name="44444444-4444-4444-4444-444444444444">
            <s:dict>
              <s:key name="host_port_pair">myserver.splunk.com:6434</s:key>
              <s:key name="peer">PEER4</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="pending_generation_id">6</s:key>
      <s:key name="pending_last_attempt">0</s:key>
      <s:key name="pending_last_reason"></s:key>
      <s:key name="replication_factor_met">1</s:key>
      <s:key name="search_factor_met">1</s:key>
      <s:key name="was_forced">0</s:key>
    </s:dict>
  </content>
</entry>
```

cluster/manager/ha_active_status

`https://<host>:<mPort>/services/cluster/manager/ha_active_status`

Used by the load balancers to check the high availability mode of a given cluster manager.

The active cluster manager will return "HTTP 200", denoting "healthy", and a startup or standby cluster manager will return "HTTP 503".

Authentication and authorization

This endpoint is unauthenticated because some load balancers don't support authentication on a health check endpoint.

GET

```
Checks the high availability mode of a given cluster manager.
```

Request parameters

None

Returned values

None

Example request and response

Request

```
curl -k -v -u admin:changeme https://mrt:15511/services/cluster/manager/ha_active_status
```

Response

From active cluster manager:

```
< HTTP/1.1 200 OK
< Date: Tue, 10 May 2022 10:45:57 GMT
< Expires: Thu, 26 Oct 1978 00:00:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, max-age=0
< Content-Type: text/xml; charset=UTF-8
< X-Content-Type-Options: nosniff
< Content-Length: 1740
< Connection: Keep-Alive
< X-Frame-Options: SAMEORIGIN
< Server: Splunkd
<
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf [httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . .-->
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>clusteractivemanager</title>
  <id>https://mrt:15511/services/cluster/manager/ha_active_status</id>
  <updated>2022-05-10T10:45:57+00:00</updated>
  <generator build="5ca3c0f7da3fe0b8be8e4a9ca6ac785dcf812149" version="20220426"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

From standby cluster manager:

```
< HTTP/1.1 503 Service Unavailable
< Date: Tue, 10 May 2022 10:47:00 GMT
< Expires: Thu, 26 Oct 1978 00:00:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, max-age=0
< Content-Type: text/xml; charset=UTF-8
< X-Content-Type-Options: nosniff
< Content-Length: 154
< Connection: Keep-Alive
< X-Frame-Options: SAMEORIGIN
< Server: Splunkd
<
<?xml version="1.0" encoding="UTF-8"?>
<response>
  <messages>
    <msg type="ERROR">Cluster manager is in inactive mode.</msg>
  </messages>
</response>
```

cluster/manager/health

`https://<host>:<mPort>/services/cluster/manager/health`

Performs health checks to determine the cluster health and search impact, prior to a rolling upgrade of the indexer cluster.

Authentication and Authorization

Requires the `admin` role or `list_indexer_cluster` capability.

GET

Get indexer cluster health check results.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Datatype	Description
all_data_is_searchable	Boolean	Indicates if all data in the cluster is searchable.
all_peers_are_up	Boolean	Indicate if all peers are strictly in the Up status.
cm_version_is_compatible	Boolean	Indicates if any cluster peers are running a Splunk Enterprise version greater than or equal to the cluster manager's version.
multisite	Boolean	Indicates if multisite is enabled.
no_fixups_in_progress	Boolean	Indicates if there does not exist buckets with bucket state `NonStreamingTarget`, or bucket search states `PendingSearchable` or `SearchablePendingMask`.
pre_flight_check	Boolean	Indicates if the health check prior to a rolling upgrade was successful. This value is true only if the cluster passed all health checks.
replication_factor_met	Boolean	Only valid for mode=manager and multisite=false. Indicates whether the replication factor is met. If true, the cluster has at least `replication_factor` number of raw data copies in the cluster.
search_factor_met	Boolean	Only valid for mode=manager and multisite=false. Indicates whether the search factor is met. If true, the cluster has at least `search_factor` number of raw data copies in the cluster.
site_replication_factor_met	Boolean	Only valid for mode=manager and multisite=true. Indicates whether the site replication factor is met. If true, the cluster has at least `replication_factor` number of raw data copies in the cluster.
site_search_factor_met	Boolean	Only valid for mode=manager and multisite=true. Indicates whether the site search factor is met. If true, the cluster has at least `site_search_factor` number of raw data copies in the cluster.
splunk_version_peer_count	String	Lists the number of cluster peers running each Splunk Enterprise version.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/health
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>clustermanagerhealth</title>
  <id>https://10.141.65.179:52000/services/cluster/manager/health</id>
  <updated>2018-04-01T19:53:47+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/health/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>manager</title>
    <id>https://10.141.65.179:52000/services/cluster/manager/health/manager</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/cluster/manager/health/manager" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/cluster/manager/health/manager" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="all_data_is_searchable">1</s:key>
        <s:key name="all_peers_are_up">1</s:key>
        <s:key name="cm_version_is_compatible">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="multisite">0</s:key>
        <s:key name="no_fixup_tasks_in_progress">1</s:key>
        <s:key name="pre_flight_check">1</s:key>
        <s:key name="replication_factor_met">1</s:key>
        <s:key name="search_factor_met">1</s:key>
        <s:key name="site_replication_factor_met">1</s:key>
        <s:key name="site_search_factor_met">1</s:key>
        <s:key name="splunk_version_peer_count">{ 7.1.0: 3 }</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

cluster/manager/indexes

`https://<host>:<mPort>/services/cluster/manager/indexes`

Access cluster index information.

GET

List cluster indices.

Request parameters

None

Returned values

Attribute	Description
buckets_with_excess_copies	Number of distinct buckets that have one or more excess replication copies.
buckets_with_excess_searchable_copies	Number of distinct buckets that have one or more excess searchable copies.
index_size	Size of the index
is_searchable	When every bucket in the index has a primary, the index is considered "searchable".
non_site_aware_buckets_in_site_aware_cluster	Number of buckets created when the cluster was not in a multisite config. (Included only when the cluster is in multisite config.)
num_buckets	Total number of distinct buckets.
replicated_copies_tracker	Displays how many distinct buckets have *X* number of copies. One of the following options. actual_copies_per_slot Number of buckets with *X* copies. expected_total_per_slot Expected number of buckets with *X* copies.
searchable_copies_tracker	Displays how many distinct buckets have *X* number of searchable copies. One of the following options. actual_copies_per_slot Number of buckets with *X* searchable copies. expected_total_per_slot Expected number of buckets with *X* searchable copies.
sort_order	Used by UI.
total_excess_bucket_copies	Total number of excess copies for all buckets.
total_excess_searchable_copies	Total number of excess searchable copies for all buckets.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/indexes
```

XML Response

```
<title>clustermanagerpeerindexes</title>
 <id>https://localhost:8089/services/cluster/manager/indexes</id>
 <updated>2014-04-17T19:11:14+00:00</updated>
 <generator build="204899" version="6.1"/>
 <author>
```

```
  <name>Splunk</name>
</author>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>_audit</title>
  <id>https://localhost:8089/services/cluster/manager/indexes/_audit</id>
  <updated>2014-04-17T19:11:14+00:00</updated>
  <link href="/services/cluster/manager/indexes/_audit" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/indexes/_audit" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="buckets_with_excess_copies">0</s:key>
      <s:key name="buckets_with_excess_searchable_copies">0</s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="index_size">284975</s:key>
      <s:key name="is_searchable">1</s:key>
      <s:key name="non_site_aware_buckets_in_site_aware_cluster">6</s:key>
      <s:key name="num_buckets">12</s:key>
      <s:key name="replicated_copies_tracker">
        <s:dict>
          <s:key name="0">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="1">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="2">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="searchable_copies_tracker">
        <s:dict>
          <s:key name="0">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="1">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="sort_order">4294967295</s:key>
      <s:key name="total_excess_bucket_copies">0</s:key>
      <s:key name="total_excess_searchable_copies">0</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>_internal</title>
  <id>https://localhost:8089/services/cluster/manager/indexes/_internal</id>
  <updated>2014-04-17T19:11:14+00:00</updated>
  <link href="/services/cluster/manager/indexes/_internal" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/indexes/_internal" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="buckets_with_excess_copies">0</s:key>
      <s:key name="buckets_with_excess_searchable_copies">0</s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="index_size">1190869</s:key>
      <s:key name="is_searchable">1</s:key>
      <s:key name="non_site_aware_buckets_in_site_aware_cluster">6</s:key>
      <s:key name="num_buckets">12</s:key>
      <s:key name="replicated_copies_tracker">
        <s:dict>
          <s:key name="0">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="1">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="2">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="searchable_copies_tracker">
        <s:dict>
          <s:key name="0">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="1">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="sort_order">4294967295</s:key>
      <s:key name="total_excess_bucket_copies">0</s:key>
      <s:key name="total_excess_searchable_copies">0</s:key>
    </s:dict>
  </content>
</entry>
```

cluster/manager/indexes/{name}

`https://<host>:<mPort>/services/cluster/manager/indexes/{name}`
Access specific cluster index information.

GET

List {name} index information.

Request parameters

None

Returned values

Attribute	Description
buckets_with_excess_copies	Number of distinct buckets that have one or more excess replication copies.
buckets_with_excess_searchable_copies	Number of distinct buckets that have one or more excess searchable copies.
index_size	Size of the index
is_searchable	When every bucket in the index has a primary, the index is considered "searchable".
non_site_aware_buckets_in_site_aware_cluster	Number of buckets created when the cluster was not in a multisite config. (Included only when the cluster is in multisite config.)
num_buckets	Total number of distinct buckets. Displays how many distinct buckets have *X* number of copies. One of the following options. actual_copies_per_slot Number of buckets with *X* copies. expected_total_per_slot Expected number of buckets with *X* copies.
searchable_copies_tracker	Displays how many distinct buckets have *X* number of searchable copies. One of the following options. actual_copies_per_slot Number of buckets with *X* searchable copies.

Attribute	Description
	expected_total_per_slot Expected number of buckets with *X* searchable copies.
sort_order	Used by UI.
total_excess_bucket_copies	Total number of excess copies for all buckets.
total_excess_searchable_copies	Total number of excess searchable copies for all buckets.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/indexes/_audit
```

XML Response

```
<title>clustermanagerpeerindexes</title>
 <id>https://localhost:8089/services/cluster/manager/indexes</id>
 <updated>2014-04-17T19:11:14+00:00</updated>
 <generator build="204899" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>2</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>_audit</title>
   <id>https://localhost:8089/services/cluster/manager/indexes/_audit</id>
   <updated>2014-04-17T19:11:14+00:00</updated>
   <link href="/services/cluster/manager/indexes/_audit" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/indexes/_audit" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="buckets_with_excess_copies">0</s:key>
       <s:key name="buckets_with_excess_searchable_copies">0</s:key>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="index_size">284975</s:key>
       <s:key name="is_searchable">1</s:key>
       <s:key name="non_site_aware_buckets_in_site_aware_cluster">6</s:key>
       <s:key name="num_buckets">12</s:key>
       <s:key name="replicated_copies_tracker">
         <s:dict>
           <s:key name="0">
             <s:dict>
               <s:key name="actual_copies_per_slot">12</s:key>
               <s:key name="expected_total_per_slot">12</s:key>
             </s:dict>
           </s:key>
           <s:key name="1">
             <s:dict>
```

```
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="2">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="searchable_copies_tracker">
        <s:dict>
          <s:key name="0">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
          <s:key name="1">
            <s:dict>
              <s:key name="actual_copies_per_slot">12</s:key>
              <s:key name="expected_total_per_slot">12</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="sort_order">4294967295</s:key>
      <s:key name="total_excess_bucket_copies">0</s:key>
      <s:key name="total_excess_searchable_copies">0</s:key>
    </s:dict>
  </content>
</entry>
```

cluster/manager/info

`https://<host>:<mPort>/services/cluster/manager/info`
Access information about cluster manager node.

GET

List cluster manager node details.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description

Name	Description
active_bundle	Provides information about the active bundle for this manager.
bundle_creation_time_on_manager	The time, in epoch seconds, when the bundle was created on the manager.
bundle_validation_errors_on_manager	A list of bundle validation errors.
bundle_validation_in_progress	Indicates if bundle validation is in progress.
bundle_validation_on_manager_succeeded	Indicates whether the manager succeeded validating bundles.
data_safety_buckets_to_fix	Lists the buckets to fix for the completion of data safety.
gen_commit_buckets_to_fix	The buckets to be fixed before the next generation can be committed.
indexing_ready_flag	Indicates if the cluster is ready for indexing.
initialized_flag	Indicates if the cluster is initialized.
label	The name for the manager. Displayed in the Splunk Web manager page.
latest_bundle	The most recent information reflecting any changes made to the manager-apps configuration bundle. In steady state, this is equal to active_bundle. If it is not equal, then pushing the latest bundle to all peers is in process (or needs to be started).
maintenance_mode	Indicates if the cluster is in maintenance mode.
reload_bundle_issued	Indicates if the bundle issued is being reloaded.
rep_count_buckets_to_fix	Number of buckets to fix on peers.
rolling_restart_flag	Indicates whether the manager is restarting the peers in a cluster.
search_count_buckets_to_fix	Number of buckets to fix to satisfy the search count.
service_ready_flag	Indicates whether the manager is ready to begin servicing, based on whether it is initialized.
start_time	Timestamp corresponding to the creation of the manager.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/info
```

XML Response

```
<title>clustermanagerinfo</title>
 <id>http://greentea.sv.splunk.com:8089/services/cluster/manager/info</id>
 <updated>2013-07-23T10:36:35-07:00</updated>
 <generator build="172635" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>manager</title>
   <id>http://greentea.sv.splunk.com:8089/services/cluster/manager/info/manager</id>
   <updated>2013-07-23T10:36:35-07:00</updated>
   <link href="/services/cluster/manager/info/manager" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/info/manager" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="active_bundle">
         <s:dict>
           <s:key
name="bundle_path">/home/eserv/schoi/apple_manager/splunk/var/run/splunk/cluster/remote-bundle
/66e383cafa8ff1f033e2341e35fc2e09-1374594357.bundle</s:key>
           <s:key name="checksum">a98f211c7bc6b141bd4fe5775c7cd193</s:key>
           <s:key name="timestamp">1374594357</s:key>
         </s:dict>
       </s:key>
       <s:key name="bundle_creation_time_on_manager">1374594357</s:key>
       <s:key name="bundle_validation_errors_on_manager">
         <s:list/>
       </s:key>
       <s:key name="bundle_validation_in_progress">0</s:key>
       <s:key name="bundle_validation_on_manager_succeeded">1</s:key>
       <s:key name="data_safety_buckets_to_fix">
         <s:dict>
           <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
             <s:dict>
               <s:key name="initial">
                 <s:dict>
                   <s:key name="reason">resolved initial state</s:key>
                   <s:key name="timestamp">1374594631</s:key>
                 </s:dict>
               </s:key>
               <s:key name="latest">
                 <s:dict>
                   <s:key name="reason"></s:key>
                   <s:key name="timestamp">1374600995</s:key>
                 </s:dict>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
             <s:dict>
               <s:key name="initial">
                 <s:dict>
                   <s:key name="reason">resolved initial state</s:key>
                   <s:key name="timestamp">1374594631</s:key>
                 </s:dict>
               </s:key>
               <s:key name="latest">
                 <s:dict>
                   <s:key name="reason"></s:key>
                   <s:key name="timestamp">1374600995</s:key>
                 </s:dict>
               </s:key>
             </s:dict>
           </s:key>
               .
               .
               .
             elided
               .
               .
```

```
        .
    <s:key name="i5~659~8CEAE4B4-BAB0-415E-9DA6-0438ECD8B3EF">
      <s:dict>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">streaming success</s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason">streaming success</s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:key>
... eai:acl node elided ...
<s:key name="gen_commit_buckets_to_fix">
  <s:dict>
    <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
      <s:dict>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">resolved initial state</s:key>
            <s:key name="timestamp">1374594631</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason"></s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
      <s:dict>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">resolved initial state</s:key>
            <s:key name="timestamp">1374594631</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason"></s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
        .
        .
        .
      elided
        .
        .
        .
    <s:key name="i5~659~8CEAE4B4-BAB0-415E-9DA6-0438ECD8B3EF">
```

```
             <s:dict>
               <s:key name="initial">
                 <s:dict>
                   <s:key name="reason">streaming success</s:key>
                   <s:key name="timestamp">1374600995</s:key>
                 </s:dict>
               </s:key>
               <s:key name="latest">
                 <s:dict>
                   <s:key name="reason">streaming success</s:key>
                   <s:key name="timestamp">1374600995</s:key>
                 </s:dict>
               </s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="indexing_ready_flag">1</s:key>
       <s:key name="initialized_flag">1</s:key>
       <s:key name="label">manager_nc</s:key>
       <s:key name="latest_bundle">
         <s:dict>
           <s:key
name="bundle_path">/home/eserv/schoi/apple_manager/splunk/var/run/splunk/cluster/remote-bundle
/66e383cafa8ff1f033e2341e35fc2e09-1374594357.bundle</s:key>
           <s:key name="checksum">a98f211c7bc6b141bd4fe5775c7cd193</s:key>
           <s:key name="timestamp">1374594357</s:key>
         </s:dict>
       </s:key>
       <s:key name="maintenance_mode">0</s:key>
       <s:key name="reload_bundle_issued">0</s:key>
       <s:key name="rep_count_buckets_to_fix">
         <s:dict>
           <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
             <s:dict>
               <s:key name="initial">
                 <s:dict>
                   <s:key name="reason">resolved initial state</s:key>
                   <s:key name="timestamp">1374594631</s:key>
                 </s:dict>
               </s:key>
               <s:key name="latest">
                 <s:dict>
                   <s:key name="reason"></s:key>
                   <s:key name="timestamp">1374600995</s:key>
                 </s:dict>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
             <s:dict>
               <s:key name="initial">
                 <s:dict>
                   <s:key name="reason">resolved initial state</s:key>
                   <s:key name="timestamp">1374594631</s:key>
                 </s:dict>
               </s:key>
               <s:key name="latest">
                 <s:dict>
                   <s:key name="reason"></s:key>
                   <s:key name="timestamp">1374600995</s:key>
                 </s:dict>
```

```
        </s:key>
      </s:dict>
    </s:key>
        .
        .
        .
      elided
        .
        .
        .
    <s:key name="i5~659~8CEAE4B4-BAB0-415E-9DA6-0438ECD8B3EF">
      <s:dict>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">streaming success</s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason">streaming success</s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:key>
<s:key name="rolling_restart_flag">0</s:key>
<s:key name="search_count_buckets_to_fix">
  <s:dict>
    <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
      <s:dict>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">resolved initial state</s:key>
            <s:key name="timestamp">1374594631</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason"></s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
      <s:dict>
        <s:key name="initial">
          <s:dict>
            <s:key name="reason">resolved initial state</s:key>
            <s:key name="timestamp">1374594631</s:key>
          </s:dict>
        </s:key>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason"></s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
```

```
          </s:key>
              .
              .
              .
            elided
              .
              .
              .
          <s:key name="i5~659~8CEAE4B4-BAB0-415E-9DA6-0438ECD8B3EF">
            <s:dict>
              <s:key name="initial">
                <s:dict>
                  <s:key name="reason">streaming success</s:key>
                  <s:key name="timestamp">1374600995</s:key>
                </s:dict>
              </s:key>
              <s:key name="latest">
                <s:dict>
                  <s:key name="reason">streaming success</s:key>
                  <s:key name="timestamp">1374600995</s:key>
                </s:dict>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="service_ready_flag">1</s:key>
      <s:key name="start_time">1374594571</s:key>
    </s:dict>
  </content>
</entry>
```

cluster/manager/peers

`https://<host>:<mPort>/services/cluster/manager/peers`
Access cluster manager peers.

See also

cluster/manager/control/control/remove_peers

GET

List cluster manager peers.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description

active_bundle_id	The ID of the configuration bundle currently being used by the manager.
apply_bundle_status	Bundle status enumeration.
base_generation_id	The initial bundle generation ID recognized by this peer. Any searches from previous generations fail. The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the manager.
bucket_count	Count of the number of buckets on this peer, across all indexes.
bucket_count_by_index	Count of the number of buckets by index on this peer.
delayed_buckets_to_discard	List of bucket IDs waiting to be discarded on this peer.
fixup_set	The set of buckets that need repair once you take the peer offline.
heartbeat_started	Flag indicating if this peer has started heartbeating.
host_port_pair	The host and port advertised to peers for the data replication channel. Can be either of the form IP:port or hostname:port.
is_searchable	Flag indicating if this peer belongs to the current committed generation and is searchable.
label	The name for the peer. Displayed on the manager page.
last_heartbeat	Timestamp for last heartbeat recieved from the peer.
latest_bundle_id	The ID of the configuration bundle this peer is using.
pending_job_count	Used by the manager to keep track of pending jobs requested by the manager to this peer.
primary_count	Number of buckets for which the peer is primary in its local site, or the number of buckets that return search results from same site as the peer.
primary_count_remote	Number of buckets for which the peer is primary that are not in its local site.
replication_count	Number of replications this peer is part of, as either source or target.
replication_port	TCP port to listen for replicated data from another cluster member.
replication_use_ssl	Indicates whether to use SSL when sending replication data.
search_state_counter	Lists the number of buckets on the peer for each search state for the bucket. Possible values for search state include: Searchable Unsearchable
site	To which site the peer belongs.
status	Indicates the status of the peer. Valid values are: Up Pending AutomaticDetention ManualDetention-PortsEnabled ManualDetention

```
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/peers/238C3311-F0A4-4A9B-97F0-53667CFFEEAB" rel="list"/>
  <link href="/services/cluster/manager/peers/238C3311-F0A4-4A9B-97F0-53667CFFEEAB" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="active_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
      <s:key name="apply_bundle_status">
        <s:dict>
          <s:key name="invalid_bundle">
            <s:dict>
              <s:key name="bundle_validation_errors">
                <s:list/>
              </s:key>
              <s:key name="invalid_bundle_id"></s:key>
            </s:dict>
          </s:key>
          <s:key name="reload_error"></s:key>
          <s:key name="restart_required_for_apply_bundle">0</s:key>
        </s:dict>
      </s:key>
      <s:key name="base_generation_id">6</s:key>
      <s:key name="bucket_count">10</s:key>
      <s:key name="bucket_count_by_index">
        <s:dict>
          <s:key name="_audit">5</s:key>
          <s:key name="_internal">5</s:key>
        </s:dict>
      </s:key>
      <s:key name="delayed_buckets_to_discard">
        <s:list/>
      </s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="fixup_set">
        <s:list/>
      </s:key>
      <s:key name="heartbeat_started">1</s:key>
      <s:key name="host_port_pair">127.0.1.1:8096</s:key>
      <s:key name="is_searchable">1</s:key>
      <s:key name="label">s2p3</s:key>
      <s:key name="last_heartbeat">1397762228</s:key>
      <s:key name="latest_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
      <s:key name="pending_job_count">0</s:key>
      <s:key name="primary_count">5</s:key>
      <s:key name="primary_count_remote">2</s:key>
      <s:key name="replication_count">0</s:key>
      <s:key name="replication_port">9905</s:key>
      <s:key name="replication_use_ssl">0</s:key>
      <s:key name="search_state_counter">
        <s:dict>
          <s:key name="Searchable">5</s:key>
          <s:key name="SearchablePendingMask">0</s:key>
          <s:key name="Unsearchable">5</s:key>
        </s:dict>
      </s:key>
      <s:key name="site">site2</s:key>
      <s:key name="status">Up</s:key>
      <s:key name="status_counter">
        <s:dict>
          <s:key name="Complete">6</s:key>
          <s:key name="NonStreamingTarget">0</s:key>
          <s:key name="StreamingSource">2</s:key>
          <s:key name="StreamingTarget">2</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
```

Name	Description

```
</entry>
    .
    .
    .
  elided
    .
    .
    .
<entry>
  <title>E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</title>
  <id>https://localhost:8089/services/cluster/manager/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</id>
  <updated>2014-04-17T19:17:08+00:00</updated>
  <link href="/services/cluster/manager/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="list"/>
  <link href="/services/cluster/manager/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="active_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
      <s:key name="apply_bundle_status">
        <s:dict>
          <s:key name="invalid_bundle">
            <s:dict>
              <s:key name="bundle_validation_errors">
                <s:list/>
              </s:key>
              <s:key name="invalid_bundle_id"></s:key>
            </s:dict>
          </s:key>
          <s:key name="reload_error"></s:key>
          <s:key name="restart_required_for_apply_bundle">0</s:key>
        </s:dict>
      </s:key>
      <s:key name="base_generation_id">4</s:key>
      <s:key name="bucket_count">13</s:key>
      <s:key name="bucket_count_by_index">
        <s:dict>
          <s:key name="_audit">6</s:key>
          <s:key name="_internal">7</s:key>
        </s:dict>
      </s:key>
      <s:key name="delayed_buckets_to_discard">
        <s:list/>
      </s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="fixup_set">
        <s:list/>
      </s:key>
      <s:key name="heartbeat_started">1</s:key>
      <s:key name="host_port_pair">127.0.1.1:8094</s:key>
      <s:key name="is_searchable">1</s:key>
      <s:key name="label">s2p1</s:key>
      <s:key name="last_heartbeat">1397762227</s:key>
      <s:key name="latest_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
      <s:key name="pending_job_count">0</s:key>
      <s:key name="primary_count">7</s:key>
      <s:key name="primary_count_remote">2</s:key>
      <s:key name="replication_count">0</s:key>
```

```
        <s:key name="replication_port">9903</s:key>
        <s:key name="replication_use_ssl">0</s:key>
        <s:key name="search_state_counter">
          <s:dict>
            <s:key name="PendingSearchable">0</s:key>
            <s:key name="Searchable">10</s:key>
            <s:key name="SearchablePendingMask">0</s:key>
            <s:key name="Unsearchable">3</s:key>
          </s:dict>
        </s:key>
        <s:key name="site">site2</s:key>
        <s:key name="status">Up</s:key>
        <s:key name="status_counter">
          <s:dict>
            <s:key name="Complete">6</s:key>
            <s:key name="NonStreamingTarget">0</s:key>
            <s:key name="StreamingSource">2</s:key>
            <s:key name="StreamingTarget">5</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

cluster/manager/peers/{name}

`https://<host>:<mPort>/services/cluster/manager/peers/{name}`

Access specified peer.

GET

Get `{name}` peer information.

Request parameters

Name	Type	Description
list_buckets	Boolean	Indicates whether to list the buckets for the peers to this manager.

Returned values

Name	Description
active_bundle_id	The ID of the configuration bundle currently being used by the manager.
apply_bundle_status	Bundle status enumeration.
base_generation_id	The initial bundle generation ID recognized by this peer. Any searches from previous generations fail. The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the manager.
bucket_count	Count of the number of buckets on this peer, across all indexes.

Name	Description
bucket_count_by_index	Count of the number of buckets by index on this peer.
delayed_buckets_to_discard	List of bucket IDs waiting to be discarded on this peer.
fixup_set	The set of buckets that need repair once you take the peer offline.
heartbeat_started	Flag indicating if this peer has started heartbeating.
host_port_pair	The host and port advertised to peers for the data replication channel. Can be either of the form IP:port or hostname:port.
is_searchable	Flag indicating if this peer belongs to the current committed generation and is searchable.
label	The name for the peer. Displayed on the Splunk Web manager page.
last_heartbeat	Timestamp for last heartbeat recieved from the peer.
latest_bundle_id	The ID of the configuration bundle this peer is using.
pending_job_count	Used by the manager to keep track of pending jobs requested by the manager to this peer.
primary_count	Number of buckets for which the peer is primary in its local site, or the number of buckets that return search results from same site as the peer.
primary_count_remote	Number of buckets for which the peer is primary that are not in its local site.
replication_count	Number of replications this peer is part of, as either source or target.
replication_port	TCP port to listen for replicated data from another cluster member.
replication_use_ssl	Indicates whether to use SSL when sending replication data.
search_state_counter	Lists the number of buckets on the peer for each search state for the bucket. Possible values for search state include: Searchable Unsearchable
site	To which site the peer belongs.
splunk_version	The version of Splunk that the peer is running. This will be of the form X.Y.Z where X is the major version, Y is the minor version, and Z is the maintenance version.
status	Indicates the status of the peer. Valid values are: Up Pending AutomaticDetention ManualDetention-PortsEnabled ManualDetention Restarting ShuttingDown ReassigningPrimaries Decommissioning GracefulShutdown Stopped Down BatchAdding

Name	Description
status_counter	Lists the number of buckets on the peer for each bucket status. Possible values for bucket status: Complete: complete (warm/cold) bucket NonStreamingTarget: target of replication for already completed (warm/cold) bucket PendingTruncate: bucket pending truncation PendingDiscard: bucket pending discard Standalone: bucket that is not replicated StreamingError: copy of streaming bucket where some error was encountered StreamingSource: streaming hot bucket on source side StreamingTarget: streaming hot bucket copy on target side Unset: uninitialized

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/cluster/manager/peers/29F9560E-A44A-425C-8753-1C6158B46C84
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

 <title>clustermanagerpeers</title>
 <id>https://localhost:8089/services/cluster/manager/peers</id>
 <updated>2014-04-17T19:18:19+00:00</updated>
 <generator build="204899" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/manager/peers/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>29F9560E-A44A-425C-8753-1C6158B46C84</title>
   <id>https://localhost:8089/services/cluster/manager/peers/29F9560E-A44A-425C-8753-1C6158B46C84</id>
   <updated>2014-04-17T19:18:19+00:00</updated>
   <link href="/services/cluster/manager/peers/29F9560E-A44A-425C-8753-1C6158B46C84" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/peers/29F9560E-A44A-425C-8753-1C6158B46C84" rel="list"/>
   <link href="/services/cluster/manager/peers/29F9560E-A44A-425C-8753-1C6158B46C84" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="active_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
       <s:key name="apply_bundle_status">
         <s:dict>
           <s:key name="invalid_bundle">
             <s:dict>
               <s:key name="bundle_validation_errors">
```

```
              <s:list/>
            </s:key>
            <s:key name="invalid_bundle_id"></s:key>
          </s:dict>
        </s:key>
        <s:key name="reload_error"></s:key>
        <s:key name="restart_required_for_apply_bundle">0</s:key>
      </s:dict>
    </s:key>
    <s:key name="base_generation_id">3</s:key>
    <s:key name="bucket_count">11</s:key>
    <s:key name="bucket_count_by_index">
      <s:dict>
        <s:key name="_audit">6</s:key>
        <s:key name="_internal">5</s:key>
      </s:dict>
    </s:key>
    <s:key name="delayed_buckets_to_discard">
      <s:list/>
    </s:key>
    <s:key name="eai:acl">
      ... elided ...
    </s:key>
    <s:key name="eai:attributes">
      ... elided ...
    </s:key>
    <s:key name="fixup_set">
      <s:list/>
    </s:key>
    <s:key name="heartbeat_started">1</s:key>
    <s:key name="host_port_pair">127.0.1.1:8092</s:key>
    <s:key name="is_searchable">1</s:key>
    <s:key name="label">s1p3</s:key>
    <s:key name="last_heartbeat">1397762298</s:key>
    <s:key name="latest_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
    <s:key name="pending_job_count">0</s:key>
    <s:key name="primary_count">6</s:key>
    <s:key name="primary_count_remote">2</s:key>
    <s:key name="replication_count">0</s:key>
    <s:key name="replication_port">9902</s:key>
    <s:key name="replication_use_ssl">0</s:key>
    <s:key name="search_state_counter">
      <s:dict>
        <s:key name="PendingSearchable">0</s:key>
        <s:key name="Searchable">8</s:key>
        <s:key name="SearchablePendingMask">0</s:key>
        <s:key name="Unsearchable">3</s:key>
      </s:dict>
    </s:key>
    <s:key name="site">site1</s:key>
    <s:key name="splunk_version">7.2.0</s:key>
    <s:key name="status">Up</s:key>
    <s:key name="status_counter">
      <s:dict>
        <s:key name="Complete">6</s:key>
        <s:key name="NonStreamingTarget">0</s:key>
        <s:key name="StreamingSource">2</s:key>
        <s:key name="StreamingTarget">3</s:key>
      </s:dict>
    </s:key>
  </s:dict>
</content>
```

```
 </entry>
</feed>
```

cluster/manager/redundancy

`https://<host>:<mPort>/services/cluster/manager/redundancy`

Display the details of all cluster managers participating in cluster manager redundancy, and switch the HA state of the cluster managers.

Authentication and authorization

The GET on this endpoint needs the capability `list_indexer_cluster`, and the POST on this endpoint needs the capability `edit_indexer_cluster`.

GET

Display the details of all cluster managers participating in cluster manager redundancy.

Request parameters

None

Returned values

Name	Description
active_bundle_id	The active bundle ID of the cluster, as set in the given cluster manager.
generation_id	The last committed generation ID of the cluster, as known to the given cluster manager.
ha_mode	The high availability mode of the given cluster manager.
last_heartbeat	The timestamp of the last heartbeat received from the given cluster manager. This is only applicable for the standby cluster managers. For the active cluster manager, this is set to 0. For standby cluster managers, this field reflects the valid timestamp, denoting the last time the active manager received a heartbeat from this standby cluster manager.
manager_switchover_mode	The switchover mode set in the given cluster manager.
peers_count	The number of indexer peers known to to the given cluster manager.
server_name	The configured server name of the given cluster manager.
uri	The management URI of the given cluster manager.

Example request and response

Request

```
curl -k -u admin:changeme -XGET "https://mrt:15511/services/cluster/manager/redundancy/?output_mode=json"
```

Response

```
{
   "links":{
      "create":"/services/cluster/manager/redundancy/_new"
   },
   "origin":"https://mrt:15511/services/cluster/manager/redundancy",
   "updated":"2022-01-25T08:29:41+00:00",
   "generator":{
      "build":"e578ec650c0bf4d48e84541eae3d501f6dfc688a",
      "version":"20211229"
   },
   "entry":[
      {
         "name":"7EE219C0-23A6-4E95-A599-64E0FE5E8B05",
         "id":"https://mrt:15511/services/cluster/manager/redundancy/7EE219C0-23A6-4E95-A599 -64E0FE5E8B05",
         "updated":"1970-01-01T00:00:00+00:00",
         "links":{
            "alternate":"/services/cluster/manager/redundancy/7EE219C0-23A6-4E95-A599-64E0FE5E8B05",
            "list":"/services/cluster/manager/redundancy/7EE219C0-23A6-4E95-A599-64E0FE5E8B05",
            "edit":"/services/cluster/manager/redundancy/7EE219C0-23A6-4E95-A599-64E0FE5E8B05"
         },
         "author":"system",
         "acl":{
            "app":"",
            "can_list":true,
            "can_write":true,
            "modifiable":false,
            "owner":"system",
            "perms":{
               "read":[
                  "admin",
                  "splunk-system-role"
               ],
               "write":[
                  "admin",
                  "splunk-system-role"
               ]
            },
            "removable":false,
            "sharing":"system"
         },
         "content":{
            "active_bundle_id":"075EA8FB2D1172A1A7AD9DA472C63E92",
            "eai:acl":null,
            "generation_id":"21",
            "ha_mode":"Active",
            "last_heartbeat":0,
            "manager_switchover_mode":"auto",
            "peers_count":"5",
            "server_name":"cm",
            "uri":"https://mrt:15511"
         }
      },
      {
         "name":"841BD315-21DB-4589-8813-15199DF02F1F",
         "id":"https://mrt:15511/services/cluster/manager/redundancy/841BD315-21DB-4589-8813 -15199DF02F1F",
         "updated":"1970-01-01T00:00:00+00:00",
         "links":{
            "alternate":"/services/cluster/manager/redundancy/841BD315-21DB-4589-8813-15199DF02F1F",
            "list":"/services/cluster/manager/redundancy/841BD315-21DB-4589-8813-15199DF02F1F",
            "edit":"/services/cluster/manager/redundancy/841BD315-21DB-4589-8813-15199DF02F1F"
         },
         "author":"system",
         "acl":{
            "app":"",
            "can_list":true,
            "can_write":true,
            "modifiable":false,
            "owner":"system",
            "perms":{
               "read":[
                  "admin",
                  "splunk-system-role"
               ],
               "write":[
                  "admin",
                  "splunk-system-role"
               ]
            },
            "removable":false,
            "sharing":"system"
         },
         "content":{
            "active_bundle_id":"075EA8FB2D1172A1A7AD9DA472C63E92",
            "eai:acl":null,
            "generation_id":"21",
            "ha_mode":"Standby",
            "last_heartbeat":1643099380,
            "manager_switchover_mode":"auto",
            "peers_count":"5",
            "server_name":"cm-standby2",
            "uri":"https://wimpy:14089"
         }
      }
   ],
   "paging":{
      "total":2,
      "perPage":30,
      "offset":0
   },
   "messages":[

   ]
}
```

POST

Switch the high availability state of the cluster managers.

Request parameters

□

Returned values

Name	Description
ha_mode	The resultant high availability mode of the given cluster manager after the mode change request completion.

Example request and response

Request

```
curl -k -u admin:changeme -XPOST
"https://10.16.88.2:15511/services/cluster/manager/redundancy/?output_mode=json" -d "_action=switch_mode" -d
"ha_mode=Active"
```

Response

```
{
   "links":{
      "create":"/services/cluster/manager/redundancy/_new"
   },
   "origin":"https://10.16.88.2:15511/services/cluster/manager/redundancy",
   "updated":"2021-10-14T04:15:00-07:00",
   "generator":{
      "build":"42f3134682e376e692f6e407a83b41c8dd787e9e",
      "version":"20211011"
   },
   "entry":[
      {
         "name":"0AB9404D-8670-4F26-8723-CA289A5A0E3A",
         "id":"https://10.16.88.2:15511/services/cluster/manager/redundancy/0AB9404D-8670-4F26-8723
-CA289A5A0E3A",
         "updated":"1969-12-31T16:00:00-08:00",
         "links":{
            "alternate":"/services/cluster/manager/redundancy/0AB9404D-8670-4F26-8723-CA289A5A0E3A",
            "list":"/services/cluster/manager/redundancy/0AB9404D-8670-4F26-8723-CA289A5A0E3A",
            "edit":"/services/cluster/manager/redundancy/0AB9404D-8670-4F26-8723-CA289A5A0E3A"
         },
         "author":"system",
         "acl":{
            "app":"",
            "can_list":true,
            "can_write":true,
            "modifiable":false,
            "owner":"system",
            "perms":{
               "read":[
                  "admin",
                  "splunk-system-role"
               ],
               "write":[
                  "admin",
                  "splunk-system-role"
               ]
            },
            "removable":false,
            "sharing":"system"
         },
         "content":{
            "eai:acl":null,
            "ha_mode":"Active"
         }
      }
   ],
   "paging":{
      "total":1,
      "perPage":30,
      "offset":0
   },
   "messages":[

   ]
}
```

cluster/manager/sites

`https://<host>:<mPort>/services/cluster/manager/sites`

Access cluster site information.

GET

List available cluster sites.

Request parameters

None

Returned values

Name	Description
peers	Peers list of host:port and server name.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/sites
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

 <title>clustermanagersites</title>
 <id>https://localhost:8089/services/cluster/manager/sites</id>
 <updated>2014-04-17T19:12:15+00:00</updated>
 <generator build="204899" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>2</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>site1</title>
   <id>https://localhost:8089/services/cluster/manager/sites/site1</id>
   <updated>2014-04-17T19:12:15+00:00</updated>
   <link href="/services/cluster/manager/sites/site1" rel="alternate"/>
   <author>
```

```
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/sites/site1" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="peers">
        <s:dict>
          <s:key name="29F9560E-A44A-425C-8753-1C6158B46C84">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8092</s:key>
              <s:key name="server_name">s1p3</s:key>
            </s:dict>
          </s:key>
          <s:key name="61666763-43E9-411B-9464-D80A5119EF0E">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8091</s:key>
              <s:key name="server_name">s1p2</s:key>
            </s:dict>
          </s:key>
          <s:key name="76C88808-2727-42B4-8C05-72DC44630FE4">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8090</s:key>
              <s:key name="server_name">s1p1</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>site2</title>
  <id>https://localhost:8089/services/cluster/manager/sites/site2</id>
  <updated>2014-04-17T19:12:15+00:00</updated>
  <link href="/services/cluster/manager/sites/site2" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/manager/sites/site2" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="peers">
        <s:dict>
          <s:key name="238C3311-F0A4-4A9B-97F0-53667CFFEEAB">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8096</s:key>
              <s:key name="server_name">s2p3</s:key>
            </s:dict>
          </s:key>
          <s:key name="C878FADC-513D-4BDD-BA48-F25BB82FE565">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8095</s:key>
              <s:key name="server_name">s2p2</s:key>
            </s:dict>
          </s:key>
          <s:key name="E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C">
```

```
              <s:dict>
                <s:key name="host_port_pair">127.0.1.1:8094</s:key>
                <s:key name="server_name">s2p1</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

cluster/manager/sites/{name}

```
https://<host>:<mPort>/services/cluster/manager/sites/{name}
```

Access specific cluster site information.

GET

List the {name} cluster site information.

Request parameters

None

Returned values

Name	Description
peers	Site peer reference, for each peer. Possible values include the following. host_port_pair Peer port number. server_name Peer server name.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/sites/site1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

  <title>clustermanagersites</title>
  <id>https://localhost:8089/services/cluster/manager/sites</id>
  <updated>2014-04-17T19:13:07+00:00</updated>
```

```
 <generator build="204899" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>site1</title>
   <id>https://localhost:8089/services/cluster/manager/sites/site1</id>
   <updated>2014-04-17T19:13:07+00:00</updated>
   <link href="/services/cluster/manager/sites/site1" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/manager/sites/site1" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="eai:attributes">
         ... elided ...
       </s:key>
       <s:key name="peers">
         <s:dict>
           <s:key name="29F9560E-A44A-425C-8753-1C6158B46C84">
             <s:dict>
               <s:key name="host_port_pair">127.0.1.1:8092</s:key>
               <s:key name="server_name">s1p3</s:key>
             </s:dict>
           </s:key>
           <s:key name="61666763-43E9-411B-9464-D80A5119EF0E">
             <s:dict>
               <s:key name="host_port_pair">127.0.1.1:8091</s:key>
               <s:key name="server_name">s1p2</s:key>
             </s:dict>
           </s:key>
           <s:key name="76C88808-2727-42B4-8C05-72DC44630FE4">
             <s:dict>
               <s:key name="host_port_pair">127.0.1.1:8090</s:key>
               <s:key name="server_name">s1p1</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
     </s:dict>
   </content>
 </entry>
</feed>
```

cluster/manager/status

`https://<host>:<mPort>/services/cluster/manager/status`

Endpoint to get the status of a rolling restart.

GET

Get the status of a rolling restart.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
decommission_force_timeout	The amount of time, in seconds, the cluster manager will wait for a peer in primary decommission status to finish primary reassignment and restart, during a searchable rolling restart with timeouts. Only valid for `rolling_restart=searchable_force`. Default value is 180. Max accepted value is 1800.
maintenance_mode	Indicates if the cluster is in maintenance mode. Happens during rolling restart, bundle push, and other maintenance activities.
messages	Array of messages from server.
multisite	Indicates if multisite is enabled for this manager. Make sure you set site parameters on the peers if you set this to true. Defaults to false.
peers	Object containing all the peers in the cluster. For each peer, the label, site and status are provided.
restart_inactivity_timeout	The amount of time, in seconds, that the manager waits for a peer to restart and rejoin the cluster before it considers the restart a failure and proceeds to restart other peers. A value of zero (0) means that the manager waits indefinitely for a peer to restart. Only valid for `rolling_restart=searchable_force`. Default is 600secs.
restart_progress	Object containing lists of peers in "done", "failed", "in_progress" and "to_be_restarted" state.
rolling_restart_flag	Boolean that indicates if there is a rolling restart in progress.
rolling_restart_or_upgrade	Boolean that indicates if there is a rolling restart or rolling upgrade in progress.
searchable_rolling	Boolean that indicates if a searchable rolling restart/upgrade in progress.
service_ready_flag	Boolean that indicates if the cluster is ready.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/manager/status
```

XML Response

```
<title>clustermanagerstatus</title>
  <id>https://10.141.65.179:52000/services/cluster/manager/status</id>
  <updated>2018-04-01T23:00:53+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/manager/status/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>manager</title>
    <id>https://10.141.65.179:52000/services/cluster/manager/status/manager</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/cluster/manager/status/manager" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/cluster/manager/status/manager" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="decommission_force_timeout">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="maintenance_mode">0</s:key>
        <s:key name="messages"></s:key>
        <s:key name="multisite">0</s:key>
        <s:key name="peers">
          <s:dict>
            <s:key name="08696C19-548F-4563-BA53-2A18769091DB">
              <s:dict>
                <s:key name="label">idx3</s:key>
                <s:key name="site">default</s:key>
                <s:key name="status">Up</s:key>
              </s:dict>
            </s:key>
            <s:key name="15FE1639-DDEF-4C50-B5A8-3E1C859FA1EA">
              <s:dict>
                <s:key name="label">idx2</s:key>
                <s:key name="site">default</s:key>
```

```
                <s:key name="status">Up</s:key>
              </s:dict>
            </s:key>
            <s:key name="73CA8A90-EC43-466F-8D12-A55C6E2EBC05">
              <s:dict>
                <s:key name="label">idx1</s:key>
                <s:key name="site">default</s:key>
                <s:key name="status">Up</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="restart_inactivity_timeout">0</s:key>
        <s:key name="restart_progress">
          <s:dict>
            <s:key name="done">
              <s:list/>
            </s:key>
            <s:key name="failed">
              <s:list/>
            </s:key>
            <s:key name="in_progress">
              <s:list/>
            </s:key>
            <s:key name="to_be_restarted">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="rolling_restart_flag">0</s:key>
        <s:key name="rolling_restart_or_upgrade">0</s:key>
        <s:key name="searchable_rolling">0</s:key>
        <s:key name="service_ready_flag">1</s:key>
      </s:dict>
    </content>
  </entry>
```

cluster/searchhead/generation

`https://<host>:<mPort>/services/cluster/searchhead/generation`
Access peer information in a cluster searchhead.

GET

List peers available to a cluster searchhead.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
generation_id	The current generation ID for this searchhead, which is part of a cluster configuration. The search head uses this information to determine which buckets to search across.
generation_peers	List of peer nodes for the current generation in the cluster configuration for this searchhead.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/searchhead/generation
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadgeneration</title>
 <id>https://localhost:8089/services/cluster/searchhead/generation</id>
 <updated>2012-09-05T11:13:45-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>manager</title>
   <id>https://localhost:8089/services/cluster/searchhead/generation/manager</id>
   <updated>2012-09-05T11:13:45-07:00</updated>
   <link href="/services/cluster/searchhead/generation/manager" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/searchhead/generation/manager" rel="list"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       <s:key name="generation_id">2</s:key>
       <s:key name="generation_peers">
         <s:dict>
           <s:key name="2AF11DD4-1424-4A14-A522-FB9D055E9516">
             <s:dict>
               <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8389</s:key>
               <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
             </s:dict>
           </s:key>
           <s:key name="50FCDB42-E167-458D-A6A9-E4587E8F16D9">
             <s:dict>
               <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8189</s:key>
               <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
     </s:dict>
   </content>
 </entry>
</feed>
```

cluster/searchhead/generation/{name}

`https://<host>:<mPort>/services/cluster/searchhead/generation/{name}`

Access peer of the manager URI.

GET

Get `{name}` searchhead generation ID and generation peers.

Request parameters

None

Returned values

Name	Description
generation_id	The current generation ID for this searchhead, which is part of a cluster configuration. The search head uses this information to determine which buckets to search across.
generation_peers	List of peer nodes for the current generation in the cluster configuration for this searchhead.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/cluster/searchhead/generation/https%3A%252F%252Fmyserver-mbp15.sv.splunk.com%3A8989
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadgeneration</title>
 <id>https://localhost:53791/services/cluster/searchhead/generation</id>
 <updated>2012-09-07T14:11:59-07:00</updated>
 <generator build="136859" version="20120906"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>https://ronnie.splunk.com:53112</title>
   <id>https://localhost:53791/services/cluster/searchhead/generation
/https%3A%252F%252Fronnie.splunk.com%3A53112</id>
   <updated>2012-09-07T14:11:59-07:00</updated>
   <link href="/services/cluster/searchhead/generation/https%3A%252F%252Fronnie.splunk.com%3A53112"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/searchhead/generation/https%3A%252F%252Fronnie.splunk.com%3A53112"
rel="list"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       ... eai:attributes node elided ...
       <s:key name="generation_id">3</s:key>
       <s:key name="generation_peers">
         <s:dict>
           <s:key name="33333333-3333-3333-3333-333333333333">
             <s:dict>
               <s:key name="host_port_pair">10.1.42.3:53309</s:key>
               <s:key name="peer">peer3</s:key>
             </s:dict>
           </s:key>
           <s:key name="44444444-4444-4444-4444-444444444444">
             <s:dict>
               <s:key name="host_port_pair">10.1.42.3:53411</s:key>
               <s:key name="peer">peer4</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
     </s:dict>
   </content>
 </entry>
</feed>
```

cluster/searchhead/searchheadconfig

`https://<host>:<mPort>/services/cluster/searchhead/searchheadconfig`
Access cluster searchhead node configuration.

GET

List this cluster search head node configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values
None

Example request and response

XML Request

```
curl -k -u   admin:pass https://localhost:8089/services/cluster/searchhead/searchheadconfig
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadconfig</title>
 <id>https://localhost:8089/services/cluster/searchhead/searchheadconfig</id>
 <updated>2013-10-31T14:04:45-07:00</updated>
 <generator build="184661" version="20131030"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/searchhead/searchheadconfig/_new" rel="create"/>
 <link href="/services/cluster/searchhead/searchheadconfig/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>https://localhost:4567</title>
   <id>https://myserver:7588/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567<
/id>
   <updated>2013-10-31T14:04:45-07:00</updated>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="list"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567/_reload"
rel="_reload"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="edit"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="remove"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       <s:key name="manager_uri">https://localhost:4567</s:key>
       <s:key name="secret">********</s:key>
     </s:dict>
   </content>
 </entry>
</feed>
```

POST

Configure this server as a cluster searchhead node.

Request parameters

Name	Type	Description
name	String	**Required**. The URI of the manager node in the cluster.
secret	String	**Required**. Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the manager, it is not able to communicate with the manager. Corresponds to pass4SymmKey setting in server.conf.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://myserver:8089/services/cluster/searchhead/searchheadconfig -d
name=https://myserver:4567 -d secret=testsecret
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadconfig</title>
 <id>https://localhost:8089/services/cluster/searchhead/searchheadconfig</id>
 <updated>2013-10-31T14:04:45-07:00</updated>
 <generator build="184661" version="20131030"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/searchhead/searchheadconfig/_new" rel="create"/>
 <link href="/services/cluster/searchhead/searchheadconfig/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>https://localhost:4567</title>
   <id>https://myserver:8089/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567<
/id>
   <updated>2013-10-31T14:04:45-07:00</updated>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="list"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567/_reload"
rel="_reload"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="edit"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="remove"/>
   <content type="text/xml">
```

```
     <s:dict>
       ... eai:acl node elided ...
       <s:key name="manager_uri">https://localhost:4567</s:key>
       <s:key name="secret">********</s:key>
     </s:dict>
   </content>
 </entry>
</feed>
```

cluster/searchhead/searchheadconfig/{name}

`https://<host>:<mPort>/services/cluster/searchhead/searchheadconfig/{name}`

Manage node in a cluster.

DELETE

Remove node from cluster.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme  --request DELETE
https://myserver.splunk.com:8089/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Fmyserver%3A8211
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadconfig</title>
 <id>https://myserver.splunk.com:8089/services/cluster/searchhead/searchheadconfig</id>
 <updated>2013-11-05T14:34:42-08:00</updated>
 <generator build="184986" version="20131101"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/searchhead/searchheadconfig/_new" rel="create"/>
 <link href="/services/cluster/searchhead/searchheadconfig/_reload" rel="_reload"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
</feed>
```

GET

List cluster search head node configuration.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass
https://myserver.splunk.com:7588/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadconfig</title>
 <id>https://myserver.splunk.com:8089/services/cluster/searchhead/searchheadconfig</id>
 <updated>2013-11-05T14:43:00-08:00</updated>
 <generator build="184986" version="20131101"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/cluster/searchhead/searchheadconfig/_new" rel="create"/>
 <link href="/services/cluster/searchhead/searchheadconfig/_reload" rel="_reload"/>
 ... openserch nodes elided ...
 <s:messages/>
 <entry>
   <title>https://localhost:4567</title>
   <id>https://myserver.splunk.com:7588/services/cluster/searchhead/searchheadconfig
/https%3A%252F%252Flocalhost%3A4567</id>
   <updated>2013-11-05T14:43:00-08:00</updated>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="list"/>
```

```
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567/_reload"
rel="_reload"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="edit"/>
   <link href="/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567"
rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                   <s:item>splunk-system-role</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list>
               <s:item>manager_uri</s:item>
               <s:item>secret</s:item>
             </s:list>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="manager_uri">https://localhost:4567</s:key>
       <s:key name="secret">********</s:key>
     </s:dict>
   </content>
 </entry>
</feed>
```

POST

Update cluster search head node configuration.

Request parameters

Name	Type	Description
manager_uri	String	The URI of the manager node in the cluster for which this searchhead is configured.
secret	String	Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the manager, it is not able to communicate with the manager. Corresponds to pass4SymmKey setting in server.conf.

Returned values
None

cluster/peer/buckets

`https://<host>:<mPort>/services/cluster/peer/buckets`
Access cluster peers bucket configuration.

GET

List cluster peers bucket configuration.

Request parameters

Name	Type	Description
generation_id	String	The generation ID for this peer. For each generation, the manager server in a cluster configuration assigns generation IDs. A generation identifies which copies of a cluster's buckets are primary and therefore can participate in a search.

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
checksum	Used internally to identify this bucket.
earliest_time	Indicates the time of the earliest event in this bucket.
generation_id	The generation ID for this peer.
generations	A sparse list of generation id to bucket primacy for the given peer.
latest_time	Indicates the time for the latest event in this bucket.
search_state	Indicates if the bucket is `searchable` or `unsearchable`.

Name	Description
status	Indicates the status of this bucket. One of the following values. Complete The copy of this bucket contains the full complement of information. StreamingSource The copy of this bucket is sending data to peer nodes for replication. StreamingTarget The copy of this bucket is receiving replicated data. NonStreamingTarget This copy of a warm bucket replication is in progress. Once replication is complete, the status changes to Complete. StreamingError The copy of this bucket encountered errors while streaming data. PendingTruncate The manager asked the peer to truncate this copy of the bucket to a certain size and is waiting for confirmation. PendingDiscard The manager asked the peer to discard this copy of the bucket (for whatever reason, and is waiting for confirmation. Standalone A bucket in the cluster that is not replicated.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/cluster/peer/buckets
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clusterpeerbuckets</title>
 <id>https://localhost:8189/services/cluster/peer/buckets</id>
 <updated>2012-09-05T12:29:42-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>_audit~0~2AF11DD4-1424-4A14-A522-FB9D055E9516</title>
   <id>https://localhost:8189/services/cluster/peer/buckets/_audit~0~2AF11DD4-1424-4A14-A522-FB9D055E9516<
/id>
   <updated>2012-09-05T12:29:42-07:00</updated>
   <link href="/services/cluster/peer/buckets/_audit~0~2AF11DD4-1424-4A14-A522-FB9D055E9516"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/peer/buckets/_audit~0~2AF11DD4-1424-4A14-A522-FB9D055E9516" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="checksum"></s:key>
```

```
      ... eai:acl node elided ...
      <s:key name="earliest_time">1346859162</s:key>
      <s:key name="generations">
        <s:dict>
          <s:key name="0">0x0</s:key>
        </s:dict>
      </s:key>
      <s:key name="latest_time">1346859257</s:key>
      <s:key name="search_state">Searchable</s:key>
      <s:key name="status">Complete</s:key>
    </s:dict>
  </content>
 </entry>
 . . . elided ...
</feed>
```

cluster/peer/buckets/{name}

`https://<host>:<mPort>/services/cluster/peer/buckets/{name}`

Manage peer buckets.

DELETE

Remove specified bucket from peer node.

Request parameters

Name	Type	Description
bucket_id	String	**Required**. The identifier for the bucket to remove.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://myserver:8089/services/cluster/peer/buckets/_internal~58~11111111-1111-1111-1111-111111111111 -d
bucket_id="_internal~58~11111111-1111-1111-1111-111111111111"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:s="http://dev.splunk.com/ns/rest"
```

```
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clusterpeerbuckets</title>
 <id>https://myserver:8089/services/cluster/peer/buckets</id>
 <updated>2013-10-31T14:48:18-07:00</updated>
 <generator build="184661" version="20131030"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
</feed>
```

GET

List peer specified bucket information.

Request parameters

Name	Type	Description
generation_id	String	The generation ID for this peer. For each generation, the manager server in a cluster configuration assigns generation IDs. A generation identifies which copies of a cluster's buckets are primary and therefore can participate in a search.

Returned values

Name	Description
checksum	Used internally to identify this bucket.
earliest_time	Indicates the time of the earliest event in this bucket.
generation_id	The generation ID for this peer.
generations	A sparse list of generation id to bucket primacy for the given peer.
latest_time	Indicates the time for the latest event in this bucket.
search_state	Indicates if the bucket is `Searchable` or `Unsearchable`.
status	Indicates the status of this bucket. One of the following values. Complete The copy of this bucket contains the full complement of information. StreamingSource The copy of this bucket is sending data to peer nodes for replication. StreamingTarget The copy of this bucket is receiving replicated data. NonStreamingTarget This copy of a warm bucket replication is in progress. Once replication is complete, the status changes to Complete. StreamingError The copy of this bucket encountered errors while streaming data. PendingTruncate The manager asked the peer to truncate this copy of the bucket to a certain size and is waiting for confirmation. PendingDiscard

Name	Description
	The manager asked the peer to discard this copy of the bucket (for whatever reason, and is waiting for confirmation. Standalone A bucket in the cluster that is not replicated.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8189/services/cluster/peer/buckets/_audit~0~B8B5E5C6-DB26-4952-AFB1-C5EFEFFFEA31
```

XML Response

```
.
.
.
 <title>clusterpeerbuckets</title>
 <id>https://localhost:8189/services/cluster/peer/buckets</id>
 <updated>2012-09-05T12:40:43-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9</title>
   <id>https://localhost:8189/services/cluster/peer/buckets/_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9<
/id>
   <updated>2012-09-05T12:40:43-07:00</updated>
   <link href="/services/cluster/peer/buckets/_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9"
rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/peer/buckets/_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="checksum"></s:key>
       ... eai:acl node elided ...
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list/>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="earliest_time">0</s:key>
       <s:key name="generations">
```

```
         <s:dict>
           <s:key name="0">0xffffffffffffffff</s:key>
         </s:dict>
       </s:key>
       <s:key name="latest_time">0</s:key>
       <s:key name="search_state">Searchable</s:key>
       <s:key name="status">StreamingSource</s:key>
     </s:dict>
   </content>
 </entry>
```

cluster/peer/control/control/decommission

`https://<host>:<mPort>/services/cluster/peer/control/control/decommission`
Endpoint to decommission an indexer cluster peer node.

POST

Decommission a peer node.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://indexer:8089/services/cluster/peer/control/control/decommission -X POST
```

XML Response

```
  <title>clusterpeercontrol</title>
  <id>https://10.141.66.19:46772/services/cluster/peer/control</id>
  <updated>2018-04-01T21:23:46+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/peer/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/peer/control/control/re-add-peer

`https://<host>:<mPort>/services/cluster/peer/control/control/re-add-peer`

Set the peer to re-add itself to the manager. This syncs the peer's state, including its in-memory bucket state, to the manager. By default, this resets the peer's primary bucket copies and the manager reassigns them across the cluster. To keep the peer's existing primary bucket copies, use the optional `clearMasks=false` parameter.

This endpoint can be useful when the manager and the peer have a state mismatch, for example when bucket information is not in sync between them.

POST

Re-add the cluster indexer to the cluster manager.

Request parameters

Name	Type	Default	Description
clearMasks	Boolean. Use `true` or `false`.	`true`	Optional. Indicates whether the manager should reassign all primary bucket copies across all peers. The default `true` value prompts the manager to reassign all primary bucket copies across all peers. Use `false` to re-add the peer but keep the existing primary bucket copies.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/cluster/peer/control/control/re-add-peer -d
clearMasks=false -X POST
```

XML Response

```
  <title>clusterpeercontrol</title>
  <id>https://localhost:8089/services/cluster/peer/control</id>
  <updated>2015-11-06T18:08:54-08:00</updated>
  <generator build="802b4ea159bb584c629dcdb8ba57c409b1d5b7ab" version="20151030"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/peer/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

cluster/peer/control/control/set_detention_override

```
https://<host>:<mPort>/services/cluster/peer/control/control/set_manual_detention
```

Deprecated. Use `/set_manual_detention` to manage peer node manual detention mode.

cluster/peer/control/control/set_manual_detention

```
https://<host>:<mPort>/services/cluster/peer/control/control/set_manual_detention
```

If you have Splunk Enterprise, you can use this endpoint to put the peer node in manual detention mode or take the peer out of this mode. In manual detention, the peer does not serve as a replication target. Detention helps slow the growth of disk usage on the peer.

Note:

- This endpoint replaces the `/set_detention_override` endpoint.
- Starting with Splunk Enterprise software version 6.5, manual detention persists through restarts.
- For more information, see Put a peer in detention in *Managing Indexers and Clusters of Indexers*.

POST

Adjust cluster peer detention mode.

Request parameters

Name	Type	Description
manual_detention	Use one of the following values. • `off`: **Default**. Remove the indexer from the detention state. • `on`: Put the indexer in manual detention mode. Close the TCP, UDP, and HTTP Event Collector data ports. Closing the ports causes most external data indexing to stop during detention. • `on_ports_enabled`: Put the indexer in manual detention mode. Do not close the TCP, UDP, or HTTP Event Collector data ports. The peer continues to index data during detention.	Enable or disable manual detention. Opt to close data ports or leave them open when manual detention is enabled.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:password https://localhost:8089/services/cluster/peer/control/control/set_manual_detention
-d manual_detention=on
```

XML Response

```
.
.
.
<title>clusterpeercontrol</title>
<id>https://localhost:8089/services/cluster/peer/control</id>
<updated>2016-11-15T20:33:01-08:00</updated>
<generator build="f3ca72fbf1234a98e7a5af9d073ae698f2e64de6" version="20161115"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/cluster/peer/control/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

cluster/peer/info

`https://<host>:<mPort>/services/cluster/peer/info`
Access cluster peer node information.

GET

List peer information.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
active_bundle	Current bundle being used by this peer.
base_generation_id	The initial bundle generation ID recognized by this peer. Any searches from previous generations fail. The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the manager.
invalid_bundle_ids	List of bundle ids with validation errors in the peer.
is_registered	Indicates if this peer is registered with the manager in the cluster.
last_heartbeat_attempt	Timestamp for the last attempt to contact the manager.
latest_bundle	Lists information about the most recent bundle downloaded from the manager.
restart_state	Indicates whether the peer needs to be restarted to enable its cluster configuration.

Name	Description
status	Indicates the status of the peer. One of the following values. • Up • Down • Pending • Detention • Restarting • DecommAwaitingPeer • DecommFixingBuckets • Decommissioned

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/cluster/peer/info
```

XML Response

```
.
.
.
 <title>clusterpeerinfo</title>
 <id>https://localhost:8189/services/cluster/peer/info</id>
 <updated>2012-09-05T12:45:59-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>peer</title>
   <id>https://localhost:8189/services/cluster/peer/info/peer</id>
   <updated>2012-09-05T12:45:59-07:00</updated>
   <link href="/services/cluster/peer/info/peer" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/peer/info/peer" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="active_bundle">
         <s:dict>
           <s:key
name="bundle_path">/Applications/splunk-peer/var/run/splunk/cluster/remote-bundle/0f6078895127ab1f715ee78a6e1ff8a1
-1346858928.bundle</s:key>
           <s:key name="checksum">36a883f4d47af66f78531ef474349b59</s:key>
           <s:key name="timestamp">1346858928</s:key>
         </s:dict>
       </s:key>
       <s:key name="base_generation_id">2</s:key>
       ... eai:acl node elided ...
       <s:key name="invalid_bundle_ids">
         <s:list/>
       </s:key>
```

```
        <s:key name="is_registered">1</s:key>
        <s:key name="last_heartbeat_attempt">1346874358</s:key>
        <s:key name="latest_bundle">
          <s:dict>
            <s:key
name="bundle_path">/Applications/splunk-peer/var/run/splunk/cluster/remote-bundle/0f6078895127ab1f715ee78a6e1ff8a1
-1346858928.bundle</s:key>
            <s:key name="checksum">36a883f4d47af66f78531ef474349b59</s:key>
            <s:key name="timestamp">1346858928</s:key>
          </s:dict>
        </s:key>
        <s:key name="restart_state">NoRestart</s:key>
        <s:key name="status">Up</s:key>
      </s:dict>
    </content>
  </entry>
```

Search head cluster endpoints

The endpoints in this section pertain to **search head clusters**.

All endpoints contain `shcluster` in their URIs pertain to search head clusters. For more information about search head clustering architecture, see Search head clustering architecture in the *Distributed Search* manual.

replication/configuration/health

`https://<host>:<mPort>/services/replication/configuration/health`
Access configuration replication health statistics for a search head cluster.

GET

Access the configuration replication health statistics for a search head cluster.

Request parameters

Name	Type	Description
bookmark	Boolean	Use this parameter with a GET request on the captain. Set to `1` to list the most recent changesets that members pulled from the captain. A timestamp is also returned for each changeset.
check_share_baseline	Boolean	Set to `1` to check for a shared baseline among members. This parameter can be used with a request on any member, including the captain.
unpublished	Boolean	Set to `1` to check for unpublished changes on members. Use this parameter with a request on a member to check if the member has any changes that have not been pushed to the captain.

Returned values

Values returned depend on the request parameters used.

`bookmark`

Name	Description

Name	Description
[server_name]	For each [server_name] member, a changeset and timestamp are shown, indicating when the [server_name] member last pulled this set of configuration changes from the captain.

Example request and response

```
curl -k -u admin:pass https://localhost:8089/services/replication/configuration/health?bookmark=1
```

```
...
  <entry>
    <title>bookmark</title>
    <id>https://localhost:11089/services/replication/configuration/health/bookmark</id>
    <updated>2016-08-08T17:08:25-07:00</updated>
    <link href="/services/replication/configuration/health/bookmark" rel="alternate"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="https://localhost:11089">CaptainDummyOpId: Mon Aug  8 16:08:55 2016</s:key>
        <s:key name="https://localhost:8089">2d9e86111eb4a377c60563f93ea5274de8b9c438: Mon Aug  8 17:08:22
2016</s:key>
        <s:key name="https://localhost:9089">2d9e86111eb4a377c60563f93ea5274de8b9c438: Mon Aug  8 17:08:22
2016</s:key>
      </s:dict>
    </content>
  </entry>
```

check_share_baseline

Application usage

This parameter compares the baseline between the current instance, on which the GET request is made, with the baseline of other members. From each of the other members, the system retrieves the oldest changeset that is not more than 23 hours old and therefore safe from purging. The system then tries to find that changeset in the current instance's local changeset repository. If the changeset is found in the local repository, then the current instance and the member share a baseline.

Establishing a shared baseline between a captain and members is a prerequisite for successful configuration replication.

Name	Description
check_share_baseline	One of the following values is returned for each of the other members. Yes: The current instance shares a baseline with this node. No: The current instance node does not share a baseline with this node. Connection error: The current instance cannot contact this node. A warning is logged with additional details.
server_name	Name for the member whose baseline is being compared to the current instance.

Example request and response

```
curl -k -u admin:pass
```

```
https://localhost:11089/services/replication/configuration/health?check_share_baseline=1
```

```
...
  <title>health</title>
  <id>https://localhost:11089/services/replication/configuration/health</id>
  <updated>2016-08-09T15:51:06-07:00</updated>
  <generator build="99005df760a86096252bb6b287ad7a6f3149a218" version="20160805"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>https://localhost:8089</title>
    <id>https://localhost:11089/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A8089<
/id>
    <updated>2016-08-09T15:51:06-07:00</updated>
    <link href="/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A8089" rel="alternate"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="check_share_baseline">Yes</s:key>
        <s:key name="server_name">yxu-mbp15-node2</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>https://localhost:9089</title>
    <id>https://localhost:11089/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A9089<
/id>
    <updated>2016-08-09T15:51:06-07:00</updated>
    <link href="/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A9089" rel="alternate"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="check_share_baseline">Yes</s:key>
        <s:key name="server_name"> localhost-node3</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>https://localhost:11089</title>
    <id>https://localhost:11089/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A11089<
/id>
    <updated>2016-08-09T15:51:06-07:00</updated>
    <link href="/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A11089"
rel="alternate"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="check_share_baseline">Yes</s:key>
        <s:key name="server_name"> localhost-node1</s:key>
      </s:dict>
    </content>
  </entry>
...
```

unpublished

A `Number of unpublished changes` key is returned with one of the following values.

Name	Description
0	

Name	Description
	All changes on this cluster member have been pushed to the captain. There are no unpublished changes on this member.
`0 (This instance is the captain)`	This message is returned when requesting `unpublished` status on the captain. The captain is always in sync with itself, so there are no unpublished changes.
`[Number greater than 0]`	The number unpublished local changes on this member. Changes are held until the next replication occurs. The node is still healthy in this case.
`No captain is available`	The search head cluster does not currently have a captain.
`Missing common baseline with the captain`	This member might be out of sync with the captain if this message persists after several replication periods. This message can also appear during a transition period, for example, when a captain is switched or a member is manually resynced. On a healthy search head cluster, the `unpublished` value should return to a numeric value after one replication period.

Example request and response

```
curl -k -u admin:pass https://localhost:11089/services/replication/configuration/health?unpublished=1
```

```
<title>health</title>
  <id>https://localhost:8089/services/replication/configuration/health</id>
  <updated>2016-08-09T13:14:16-07:00</updated>
  <generator build="99005df760a86096252bb6b287ad7a6f3149a218" version="20160805"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>unpublished</title>
    <id>https://localhost:8089/services/replication/configuration/health/unpublished</id>
    <updated>2016-08-09T13:14:16-07:00</updated>
    <link href="/services/replication/configuration/health/unpublished" rel="alternate"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Number of unpublished changes">0</s:key>
      </s:dict>
    </content>
  </entry>
```

replication/configuration/quarantined-assets

`https://<host>:<mPort>/services/replication/configuration/quarantined-assets`

Access information about quarantined lookups in a search head cluster.

GET

Access information about quarantined lookups in a search head cluster.

Request parameters

None

Returned values

Name	Description
assetName	The name of the quarantined CSV lookup.
quarantined_at_host	The URL of the search head cluster member on which the lookup is quarantined.
quarantined_at	Seconds since epoch.
lookup_size	The size of the quarantined lookup in Bytes.

Example request and response

```
curl -k -u admin:pass https://localhost:8090/services/replication/configuration/quarantined-assets
```

```
...
  <title>quarantined-assets</title>
    <id>https://localhost:8090/services/replication/configuration/quarantined-assets/quarantined-assets<
/id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/replication/configuration/quarantined-assets/quarantined-assets" rel="alternate"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="assetId">b4c9340713a5dd8c61105b05acea79fbbd3fc98d</s:key>
        <s:key name="assetURI">/nobody/search/lookups/test.csv</s:key>
        <s:key name="user">nobody</s:key>
        <s:key name="app">search</s:key>
        <s:key name="assetType">lookups</s:key>
        <s:key name="assetName">test.csv</s:key>
        <s:key name="quarantineInfo">[ {quarantined_at_host=https://localhost:8090,
quarantined_at=1724885036, lookup_size=30246329, quarantine_reason=large_lookup} ]</s:key>
      </s:dict>
    </content>
```

shcluster/captain/artifacts

`https://<host>:<mPort>/services/shcluster/captain/artifacts`

Provides list of artifacts and replicas currently managed by the captain across a searchhead cluster.

This endpoint can only be accessed on the captain. The response lists all artifacts that are currently resident on the set of search head cluster members.

An artifact in search head clustering is a managed search directory. Currently, only scheduled search results directories are managed and replicated according to replication policy.

> **Note:** Ad hoc searches are not considered artifacts and are not listed.

GET

Lists searchhead cluster artifacts and replicas.

Request parameters

Name	Type	Description
remote_sids	Bool	**Required**. Set this to true to return the searches that the captain is seeing. Will include adhoc searches on remote members.

Returned values

Name	Description
artifact_size	Artifact size, in bytes.
origin_guid	Guid of the origin peer where this artifact was created/search was run.
peers	Lists information about replicas of this artifact on members of this searchhead cluster.
service_after_time	Artifact service/fixup is deferred until after this time.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/shcluster/captain/artifacts
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptainartifacts</title>
  <id>https://localhost:8089/services/shcluster/captain/artifacts</id>
  <updated>2014-10-15T08:44:41-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/artifacts/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:44:41-07:00</updated>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268
```

```
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="artifact_size">282624</s:key>
        ... eai:acl node elided ...
        <s:key name="origin_guid">88888888-8888-8888-8888-888888888888</s:key>
        <s:key name="peers">
          <s:dict>
            <s:key name="88888888-8888-8888-8888-888888888888">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/searchhead/var/run/splunk/dispatch/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
            <s:key name="99999999-9999-9999-9999-999999999999">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/dash/var/run/splunk/dispatch/rsa_scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="service_after_time">0</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:44:41-07:00</updated>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="artifact_size">282624</s:key>
        ... eai:acl node elided ...
        <s:key name="origin_guid">88888888-8888-8888-8888-888888888888</s:key>
        <s:key name="peers">
          <s:dict>
            <s:key name="88888888-8888-8888-8888-888888888888">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/searchhead/var/run/splunk/dispatch/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
            <s:key name="99999999-9999-9999-9999-999999999999">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/dash/var/run/splunk/dispatch/rsa_scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="service_after_time">0</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387300_288_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387300_288_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:44:41-07:00</updated>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387300_288
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387300_288
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387300_288
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="artifact_size">253952</s:key>
        ... eai:acl node elided ...
        <s:key name="origin_guid">88888888-8888-8888-8888-888888888888</s:key>
        <s:key name="peers">
          <s:dict>
            <s:key name="88888888-8888-8888-8888-888888888888">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/searchhead/var/run/splunk/dispatch/scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387300_288_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
            <s:key name="99999999-9999-9999-9999-999999999999">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/dash/var/run/splunk/dispatch/rsa_scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387300_288_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="service_after_time">0</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387600_289_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387600_289_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:44:41-07:00</updated>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387600_289
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387600_289
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387600_289
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="artifact_size">253952</s:key>
        ... eai:acl node elided ...
        <s:key name="origin_guid">88888888-8888-8888-8888-888888888888</s:key>
        <s:key name="peers">
          <s:dict>
            <s:key name="88888888-8888-8888-8888-888888888888">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/searchhead/var/run/splunk/dispatch/scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387600_289_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
            <s:key name="99999999-9999-9999-9999-999999999999">
              <s:dict>
                <s:key
name="directory_path">/home/svasan/splunk/dash/var/run/splunk/dispatch/rsa_scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387600_289_88888888-8888-8888-8888-888888888888</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="service_after_time">0</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/captain/artifacts/{name}

`https://<host>:<mPort>/services/shcluster/captain/artifacts/{name}`

Get artifact information for a specific artifact.

GET

Get artifact information, size, replicas and earliest service time.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	! Description
artifact_size	Artifact size, in bytes.
origin_guid	Guid of the origin peer where this artifact was created.
peers	Lists information about artifacts on members of this captain.
service_after_time	Artifact service is deferred until after this time.

Example request and response

XML Request

```
curl -k -u admin:pass
https://locahost:8089/services/shcluster/captain/artifacts/scheduler__nobody__simplexml__RMD5dc07327042a35a17_at
_1469214000_37_11111111-1111-1111-1111-111111111111
```

XML Response

```
  <title>shclustercaptainartifacts</title>
  <id>https://localhost:8089/services/shcluster/captain/artifacts</id>
  <updated>2016-07-22T13:39:03-07:00</updated>
  <generator build="d6d01722fce508a9e2f032d36d8d6a445b7d6292" version="20160721"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/artifacts/_new" rel="create"/>
  <link href="/services/shcluster/captain/artifacts/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler__nobody__simplexml__RMD5dc07327042a35a17_at_1469214000_37_11111111-1111-1111-1111
-111111111111</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__nobody__simplexml_
_RMD5dc07327042a35a17_at_1469214000_37_11111111-1111-1111-1111-111111111111</id>
    <updated>2016-07-22T13:39:03-07:00</updated>
    <link
href="/services/shcluster/captain/artifacts/scheduler__nobody__simplexml__RMD5dc07327042a35a17_at_1469214000_37
_11111111-1111-1111-1111-111111111111" rel="alternate"/>
    <author>
```

```
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/artifacts/scheduler__nobody__simplexml__RMD5dc07327042a35a17_at_1469214000_37
_11111111-1111-1111-1111-111111111111" rel="list"/>
    <link
href="/services/shcluster/captain/artifacts/scheduler__nobody__simplexml__RMD5dc07327042a35a17_at_1469214000_37
_11111111-1111-1111-1111-111111111111" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="artifact_size">77824</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:acl.app">simplexml</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="label">timechart_scheduled</s:key>
        <s:key name="origin_guid">11111111-1111-1111-1111-111111111111</s:key>
        <s:key name="peers">
          <s:dict>
            <s:key name="11111111-1111-1111-1111-111111111111">
              <s:dict>
                <s:key
name="directory_path">/home/user/home_1/var/run/splunk/dispatch/scheduler__nobody__simplexml__RMD5dc07327042a35a17
_at_1469214000_37_11111111-1111-1111-1111-111111111111</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
            <s:key name="33333333-3333-3333-3333-333333333333">
              <s:dict>
                <s:key
name="directory_path">/home/user/home_3/var/run/splunk/dispatch/rsa_scheduler__nobody__simplexml_
_RMD5dc07359042a35a17_at_1469214000_37_11111111-1111-1111-1111-111111111111</s:key>
                <s:key name="status">Complete</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="perms">read : [ *, splunk-system-user ], write : [ admin, power, splunk-system-user
]</s:key>
        <s:key name="service_after_time">0</s:key>
        <s:key name="user">splunk-system-user</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/captain/control/default/restart

`https://<host>:<mPort>/services/shcluster/captain/control/default/restart`

Endpoint to initiate rolling restart of a search head cluster.

POST

Initiates rolling restart of a search head cluster

Request parameters

Name	Type	Description
searchable	Boolean	Maintain high search availability during a rolling restart.
force	Boolean	Override health check failures to continue searchable rolling restart.
decommission_search_jobs_wait_secs	Integer	Maximum time in secs that searchable rolling restart waits for existing searches to finish. Default: 180 secs.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:password  https://localhost:8089/services/shcluster/captain/control/default/restart -d
searchable=1 -d force=1 -d decommission_search_jobs_wait_secs=30 -X POST
```

XML Response

```
<title>shclustercaptaincontrol</title>
  <id>https://10.222.21.58:8089/services/shcluster/captain/control</id>
  <updated>2018-03-29T12:08:09-07:00</updated>
  <generator build="d75793dbca24" version="7.1.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/control/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Restart of search head cluster members initiated.</s:msg>
  </s:messages>
  <entry>
    <title>restart</title>
    <id>https://10.222.21.58:8089/services/shcluster/captain/control/restart</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/shcluster/captain/control/restart" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/control/restart" rel="list"/>
    <link href="/services/shcluster/captain/control/restart" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="msg">Searchable rolling restarted cannot be started without captain status = Up, check
status through "splunk show shcluster-status".</s:key>
        <s:key name="success">0</s:key>
      </s:dict>
    </content>
  </entry>
```

shcluster/captain/control/control/rotate-splunk-secret

`https://<host>:<mPort>/services/shcluster/captain/control/control/rotate-splunk-secret`

Rotates the `splunk.secret` file on all nodes of a search head cluster.

POST

Rotates the `splunk.secret` file on all nodes of a search head cluster.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme
 https://localhost:8089/services/shcluster/captain/control/control/rotate-splunk-secret -X POST
```

XML Response

shcluster/captain/control/control/upgrade-init

`https://<host>:<mPort>/services/shcluster/captain/control/control/upgrade-init`

Initializes a search head cluster rolling upgrade.

POST

Initializes a search head cluster rolling upgrade.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/shcluster/captain/control/control/upgrade-init -X
POST
```

XML Response

```
  <title>shclustercaptaincontrol</title>
  <id>https://10.222.21.58:8089/services/shcluster/captain/control</id>
  <updated>2018-03-29T12:02:54-07:00</updated>
  <generator build="d75793dbca24" version="7.1.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/control/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Upgrade of search head cluster members initiated.</s:msg>
  </s:messages>
  <entry>
    <title>upgrade-init</title>
    <id>https://10.222.21.58:8089/services/shcluster/captain/control/upgrade-init</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/shcluster/captain/control/upgrade-init" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/control/upgrade-init" rel="list"/>
    <link href="/services/shcluster/captain/control/upgrade-init" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="success">1</s:key>
        <s:key name="upgrade">yes</s:key>
      </s:dict>
    </content>
  </entry>
```

shcluster/captain/control/control/upgrade-finalize

`https://<host>:<mPort>/services/shcluster/captain/control/control/upgrade-finalize`

Finishes a search head cluster rolling upgrade.

POST

Finishes a search head cluster rolling upgrade.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme
  https://localhost:8089/services/shcluster/captain/control/control/upgrade-finalize -X POST
```

XML Response

```
<title>shclustercaptaincontrol</title>
  <id>https://10.222.21.58:8089/services/shcluster/captain/control</id>
  <updated>2018-03-29T12:06:47-07:00</updated>
  <generator build="d75793dbca24" version="7.1.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/control/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Upgrade of search head cluster members finalized.</s:msg>
  </s:messages>
  <entry>
    <title>upgrade-finalize</title>
    <id>https://10.222.21.58:8089/services/shcluster/captain/control/upgrade-finalize</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/shcluster/captain/control/upgrade-finalize" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/control/upgrade-finalize" rel="list"/>
    <link href="/services/shcluster/captain/control/upgrade-finalize" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="success">1</s:key>
        <s:key name="upgrade">no</s:key>
      </s:dict>
    </content>
  </entry>
```

shcluster/captain/info

`https://<host>:<mPort>/services/shcluster/captain/info`

Access information about searchhead cluster captain node.

GET

List searchhead cluster captain node details.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
elected_captain	Time when the current captain was elected
id	Id of this SH cluster. This is used as the unique identifier for the Search Head Cluster in bundle replication and acceleration summary management.
initialized_flag	Indicates if the searchhead cluster is initialized.
label	The name for the captain. Displayed on the Splunk Web manager page.
maintenance_mode	Indicates if the cluster is in maintenance mode.
min_peers_joined_flag	Flag to indicate if more then replication_factor peers have joined the cluster.
peer_scheme_host_port	URI of the current captain.
rolling_restart_flag	Indicates whether the captain is restarting the members in a searchhead cluster.
service_ready_flag	Indicates whether the captain is ready to begin servicing, based on whether it is initialized.
start_time	Timestamp corresponding to the creation of the captain.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/info
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptaininfo</title>
  <id>https://localhost:8089/services/shcluster/captain/info</id>
  <updated>2014-10-15T08:45:25-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>captain</title>
    <id>https://localhost:8089/services/shcluster/captain/info/captain</id>
    <updated>2014-10-15T08:45:25-07:00</updated>
    <link href="/services/shcluster/captain/info/captain" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/info/captain" rel="list"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="elected_captain">1413307273</s:key>
        <s:key name="id">BB3116C0-73B9-459A-B473-254A18A69776</s:key>
        <s:key name="initialized_flag">1</s:key>
        <s:key name="label">searchhead</s:key>
        <s:key name="maintenance_mode">0</s:key>
        <s:key name="min_peers_joined_flag">1</s:key>
        <s:key name="peer_scheme_host_port">https://localhost:55569</s:key>
        <s:key name="rolling_restart_flag">0</s:key>
        <s:key name="service_ready_flag">1</s:key>
        <s:key name="start_time">1413307203</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/captain/jobs

`https://<host>:<mPort>/services/shcluster/captain/jobs`

List running and recently finished jobs for all cluster members.

GET

List running and recently finished jobs for this cluster.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

For each job:

Name	Description
ATTEMPT_[n]	*dispatch_time* - The UTC time of dispatch for the job *errormsg* - If the job failed, capturing the reason for failure *peer* - GUID of the member that the job was sent to *sid* - the search id of this attempt *success* - a boolean for success/failure of the job
job_state	Job State can be `SCHEDULED`/`DISPATCHED`/`COMPLETED`. A `SCHEDULED` job has been received by the captain from the scheduler to schedule. A `DISPATCHED` job has started to run on a remote member. A `COMPLETED` job has finished running on the remote member.
saved_search	The name of the saved-search from the associated `savedsearches.conf` file.
savedsearchtype	The scheduler manages three kinds of scheduled jobs, regular `savedsearch` for both realtime and historical, `autosummary` report acceleration build searches, and `tsidx` tsidx build searches.
search_app	The application in which the savedsearch was created.
search_owner	The owner of the saved search.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/jobs
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptainjobs</title>
  <id>https://localhost:8089/services/shcluster/captain/jobs</id>
  <updated>2014-10-15T08:47:50-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/jobs/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>savedsearch_Alert - syslog errors last hour_1087026166</title>
    <id>https://localhost:8089/services/shcluster/captain/jobs/savedsearch_Alert%20
-%20syslog%20errors%20last%20hour_1087026166</id>
    <updated>2014-10-15T08:47:50-07:00</updated>
    <link
href="/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_1087026166"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_1087026166"
rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="ATTEMPT_1">
          <s:dict>
            <s:key name="dispatch_time">1413363600</s:key>
            <s:key name="errormsg">error response peer=https://wimpy.splunk.com:55560 rc=404 reason='<?xml
version="1.0" encoding="UTF-8"?>
<response>
  <messages>
    <msg type="ERROR">Application does not exist: SA-nix</msg>
  </messages>
</response>
'</s:key>
            <s:key name="peer">99999999-9999-9999-9999-999999999999</s:key>
            <s:key name="sid">NO_SID_RECEIVED_YET</s:key>
            <s:key name="success">0</s:key>
          </s:dict>
        </s:key>
        <s:key name="ATTEMPT_2">
          <s:dict>
            <s:key name="dispatch_time">1413363600</s:key>
            <s:key name="peer">88888888-8888-8888-8888-888888888888</s:key>
            <s:key
name="sid">scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413363600_203_88888888-8888-8888-8888
-888888888888</s:key>
            <s:key name="success">1</s:key>
          </s:dict>
        </s:key>
        ... eai:acl node elided ...
        <s:key name="job_state">COMPLETED</s:key>
        <s:key name="saved_search">Alert - syslog errors last hour</s:key>
        <s:key name="savedsearchtype">savedsearch</s:key>
        <s:key name="search_app">SA-nix</s:key>
        <s:key name="search_owner">admin</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>savedsearch_Alert - syslog errors last hour_11648853</title>
    <id>https://localhost:8089/services/shcluster/captain/jobs/savedsearch_Alert%20
-%20syslog%20errors%20last%20hour_11648853</id>
    <updated>2014-10-15T08:47:50-07:00</updated>
    <link
href="/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_11648853"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_11648853"
rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="ATTEMPT_1">
          <s:dict>
            <s:key name="dispatch_time">1413316800</s:key>
            <s:key name="errormsg">error response peer=https://wimpy.splunk.com:55560 rc=404 reason='<?xml
version="1.0" encoding="UTF-8"?>
<response>
  <messages>
    <msg type="ERROR">Application does not exist: SA-nix</msg>
  </messages>
</response>
'</s:key>
            <s:key name="peer">99999999-9999-9999-9999-999999999999</s:key>
            <s:key name="sid">NO_SID_RECEIVED_YET</s:key>
            <s:key name="success">0</s:key>
          </s:dict>
        </s:key>
        <s:key name="ATTEMPT_2">
          <s:dict>
            <s:key name="dispatch_time">1413316800</s:key>
            <s:key name="peer">88888888-8888-8888-8888-888888888888</s:key>
            <s:key
name="sid">scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413316800_34_88888888-8888-8888-8888-888888888888<
/s:key>
            <s:key name="success">1</s:key>
          </s:dict>
        </s:key>
        ... eai:acl node elided ...
        <s:key name="job_state">COMPLETED</s:key>
        <s:key name="saved_search">Alert - syslog errors last hour</s:key>
        <s:key name="savedsearchtype">savedsearch</s:key>
        <s:key name="search_app">SA-nix</s:key>
        <s:key name="search_owner">admin</s:key>
      </s:dict>
    </content>
  </entry>
      .
      .
      .
<entry>
    <title>savedsearch_fired_alerts_1050236433</title>
    <id>https://localhost:8089/services/shcluster/captain/jobs/savedsearch_fired_alerts_1050236433</id>
    <updated>2014-10-15T08:47:50-07:00</updated>
    <link href="/services/shcluster/captain/jobs/savedsearch_fired_alerts_1050236433" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/jobs/savedsearch_fired_alerts_1050236433" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="ATTEMPT_1">
          <s:dict>
            <s:key name="dispatch_time">1413308100</s:key>
            <s:key name="errormsg">error response peer=https://wimpy.splunk.com:55560 rc=404 reason='<?xml
version="1.0" encoding="UTF-8"?>
<response>
  <messages>
    <msg type="ERROR">Application does not exist: SA-nix</msg>
  </messages>
</response>
'</s:key>
            <s:key name="peer">99999999-9999-9999-9999-999999999999</s:key>
            <s:key name="sid">NO_SID_RECEIVED_YET</s:key>
            <s:key name="success">0</s:key>
          </s:dict>
        </s:key>
        <s:key name="ATTEMPT_2">
          <s:dict>
            <s:key name="dispatch_time">1413308100</s:key>
            <s:key name="peer">88888888-8888-8888-8888-888888888888</s:key>
            <s:key
name="sid">scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413308100_2_88888888-8888-8888-8888-888888888888<
/s:key>
            <s:key name="success">1</s:key>
          </s:dict>
        </s:key>
        ... eai:acl node elided ...
        <s:key name="job_state">COMPLETED</s:key>
        <s:key name="saved_search">fired_alerts</s:key>
        <s:key name="savedsearchtype">savedsearch</s:key>
        <s:key name="search_app">SA-nix</s:key>
        <s:key name="search_owner">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/captain/jobs/{name}

```
https://<host>:<mPort>/services/shcluster/captain/jobs/{name}
```

GET

Get running and recently finished jobs for `{name}` cluster.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
ATTEMPT_[n]	*dispatch_time* - The UTC time of dispatch for the job *errormsg* - If the job failed, capturing the reason for failure *peer* - GUID of the member that the job was sent to *sid* - the search id of this attempt *success* - a boolean for success/failure of the job
job_state	Job State can be `SCHEDULED`/`DISPATCHED`/`COMPLETED`. A `SCHEDULED` job has been received by the captain from the scheduler to schedule. A `DISPATCHED` job has started to run on a remote member. A `COMPLETED` job has finished running on the remote member.
saved_search	The name of the saved-search from the associated `savedsearches.conf` file.
savedsearchtype	The scheduler manages three kinds of scheduled jobs, regular `savedsearch` for both realtime and historical, `autosummary` report acceleration build searches, and `tsidx` tsidx build searches.
search_app	The application in which the savedsearch was created.
search_owner	The owner of the saved search.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/jobs/scheduled
_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_12944444515
```

XML Response

```
  <title>shclustercaptainjobs</title>
  <id>https://localhost:8089/services/shcluster/captain/jobs</id>
  <updated>2016-07-22T13:56:18-07:00</updated>
  <generator build="d6d01722fce508a9e2f032d36d8d6a445b7d6292" version="20160721"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/jobs/_new" rel="create"/>
  <link href="/services/shcluster/captain/jobs/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduled_sample scheduled search for dashboards (existing job case)
timechart_1290934515</title>
    <id>https://localhost:8089/services/shcluster/captain/jobs/scheduled
_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_1290934515</id>
    <updated>2016-07-22T13:56:18-07:00</updated>
    <link href="/services/shcluster/captain/jobs/scheduled
_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_1294444515"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/jobs/scheduled
_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_12904444515"
rel="list"/>
    <link href="/services/shcluster/captain/jobs/scheduled
```

```
_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_12909444515"
rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="dispatch_time">1469214120</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="job_state">COMPLETED</s:key>
        <s:key name="peer">11111111-1111-1111-1111-111111111111</s:key>
        <s:key name="peer_scheme_host_port">https://wimpy:13221</s:key>
        <s:key name="peer_servername">home-1</s:key>
        <s:key name="saved_search">sample scheduled search for dashboards (existing job case)
timechart</s:key>
        <s:key name="savedsearchtype">scheduled</s:key>
        <s:key name="search_app">testing</s:key>
        <s:key name="search_owner">nobody</s:key>
        <s:key
name="sid">scheduler__nobody__testing__RMD5058c22ce2c07889b_at_1469214120_39_11111111-1111-1111-1111
-111111111111</s:key>
        <s:key name="success">1</s:key>
      </s:dict>
    </content>
  </entry>
```

shcluster/captain/members

`https://<host>:<mPort>/services/shcluster/captain/members`

Lists the search head cluster members.

GET

List cluster members.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
adhoc_searchhead	Flag to indicate if this member does not run scheduled searches.
advertise_restart_required	Flag to indicate if this peer advertised that it needed a restart.
artifact_count	Number of artifacts on this peer
delayed_artifacts_to_discard	List of artifacts waiting to be deleted from this peer.
fixup_set	N/A
host_port_pair	The host and management port advertised by this peer.
kv_store_host_port	Host and port of the kv store instance of this member.
label	The name for this member. Displayed on the Splunk Web manager page.
last_heartbeat	Timestamp for last heartbeat recieved from the peer
peer_scheme_host_port	URI of the current captain.
pending_job_count	Used by the captain to keep track of pending jobs requested by the captain to this member.
replication_count	Number of replications this peer is part of, as either source or target.
replication_port	TCP port to listen for replicated data from another cluster member.
replication_use_ssl	Indicates whether to use SSL when sending replication data.
site	N/A
status	Indicates the status of the member. Possible values are the following. • Up • Pending • AutomaticDetention • ManualDetention-PortsEnabled • ManualDetention • Restarting

Name	Description
	• ShuttingDown • ReassigningPrimaries • Decommissioning • GracefulShutdown • Stopped • Down • BatchAdding
status_counter	Lists the number of buckets on the peer for each bucket status. Possible values are the following. Complete Complete (warm/cold) bucket NonStreamingTarget Target of replication for already completed (warm/cold) bucket PendingTruncate Bucket pending truncation PendingDiscard Bucket pending discard Standalone Bucket that is not replicated StreamingError Copy of streaming bucket where some error was encountered StreamingSource Streaming hot bucket on source side StreamingTarget Streaming hot bucket copy on target side Unset Uninitialized

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/members
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptainmembers</title>
  <id>https://localhost:8089/services/shcluster/captain/members</id>
  <updated>2014-10-15T08:49:34-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/members/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>88888888-8888-8888-8888-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/members/88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:49:34-07:00</updated>
    <link href="/services/shcluster/captain/members/88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/members/88888888-8888-8888-8888-888888888888" rel="list"/>
    <link href="/services/shcluster/captain/members/88888888-8888-8888-8888-888888888888" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="adhoc_searchhead">0</s:key>
        <s:key name="advertise_restart_required">0</s:key>
        <s:key name="artifact_count">4</s:key>
        <s:key name="delayed_artifacts_to_discard">
          <s:list/>
        </s:key>
        ... eai:acl node elided ...
        <s:key name="fixup_set">
          <s:list/>
        </s:key>
        <s:key name="host_port_pair">localhost:8089</s:key>
        <s:key name="kv_store_host_port">?</s:key>
        <s:key name="label">searchhead</s:key>
        <s:key name="last_heartbeat">1413388171</s:key>
        <s:key name="peer_scheme_host_port">https://localhost:8089</s:key>
        <s:key name="pending_job_count">0</s:key>
        <s:key name="replication_count">0</s:key>
        <s:key name="replication_port">3456</s:key>
        <s:key name="replication_use_ssl">0</s:key>
        <s:key name="site">site2</s:key>
        <s:key name="status">Up</s:key>
        <s:key name="status_counter">
          <s:dict>
            <s:key name="Complete">4</s:key>
            <s:key name="PendingDiscard">0</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>99999999-9999-9999-9999-999999999999</title>
    <id>https://localhost:8089/services/shcluster/captain/members/99999999-9999-9999-9999-999999999999</id>
    <updated>2014-10-15T08:49:34-07:00</updated>
    <link href="/services/shcluster/captain/members/99999999-9999-9999-9999-999999999999" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/members/99999999-9999-9999-9999-999999999999" rel="list"/>
    <link href="/services/shcluster/captain/members/99999999-9999-9999-9999-999999999999" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="adhoc_searchhead">0</s:key>
        <s:key name="advertise_restart_required">0</s:key>
        <s:key name="artifact_count">4</s:key>
        <s:key name="delayed_artifacts_to_discard">
          <s:list/>
        </s:key>
        ... eai:acl node elided ...
        <s:key name="fixup_set">
          <s:list/>
        </s:key>
        <s:key name="host_port_pair">wimpy.splunk.com:55560</s:key>
        <s:key name="kv_store_host_port">?</s:key>
        <s:key name="label">manager</s:key>
        <s:key name="last_heartbeat">1413388171</s:key>
```

```
        <s:key name="peer_scheme_host_port">https://wimpy.splunk.com:55560</s:key>
        <s:key name="pending_job_count">0</s:key>
        <s:key name="replication_count">0</s:key>
        <s:key name="replication_port">55570</s:key>
        <s:key name="replication_use_ssl">0</s:key>
        <s:key name="site">site1</s:key>
        <s:key name="status">Up</s:key>
        <s:key name="status_counter">
          <s:dict>
            <s:key name="Complete">4</s:key>
            <s:key name="NonStreamingTarget">0</s:key>
            <s:key name="PendingDiscard">0</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/captain/members/{name}

`https://<host>:<mPort>/services/shcluster/captain/members/{name}`

Get information about the `{name}` searchhead cluster member.

GET

Get information about the `{name}` searchhead cluster member.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
adhoc_searchhead	Flag to indicate if this member does not run scheduled searches.
advertise_restart_required	Flag to indicate if this peer advertised that it needed a restart.
artifact_count	Number of artifacts on this peer.
delayed_artifacts_to_discard	List of artifacts waiting to be deleted from this peer.
fixup_set	N/A
host_port_pair	The host and management port advertised by this peer.
kv_store_host_port	Host and port of the kv store instance of this member.
label	The name for this member. Displayed on the Splunk Web manager page.
last_heartbeat	Timestamp for last heartbeat recieved from the peer
peer_scheme_host_port	URI of the current captain.

Name	Description
pending_job_count	Used by the manager to keep track of pending jobs requested by the manager to this peer.
replication_count	Number of replications this peer is part of, as either source or target.
replication_port	TCP port to listen for replicated data from another cluster member.
replication_use_ssl	Indicates whether to use SSL when sending replication data.
site	N/A
status	Indicates the status of the member. Possible values are the following. • Up • Pending • AutomaticDetention • ManualDetention-PortsEnabled • ManualDetention • Restarting • ShuttingDown • ReassigningPrimaries • Decommissioning • GracefulShutdown • Stopped • Down • BatchAdding
status_counter	Lists the number of buckets on the peer for each bucket status. Possible values are the following. Complete Complete (warm/cold) bucket NonStreamingTarget Target of replication for already completed (warm/cold) bucket PendingTruncate Bucket pending truncation PendingDiscard Bucket pending discard Standalone Bucket that is not replicated StreamingError Copy of streaming bucket where some error was encountered StreamingSource Streaming hot bucket on source side StreamingTarget Streaming hot bucket copy on target side Unset Uninitialized

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptainmembers</title>
  <id>https://wimpy:13221/services/shcluster/captain/members</id>
  <updated>2016-07-22T14:12:50-07:00</updated>
  <generator build="d6d01722fce508a9e2f032d36d8d6a445b7d6292" version="20160721"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/members/_new" rel="create"/>
  <link href="/services/shcluster/captain/members/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>33333333-3333-3333-3333-333333333333</title>
    <id>https://localhost:8089/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333</id>
    <updated>2016-07-22T14:12:50-07:00</updated>
    <link href="/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333" rel="list"/>
    <link href="/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="adhoc_searchhead">0</s:key>
        <s:key name="advertise_restart_required">0</s:key>
        <s:key name="artifact_count">6</s:key>
        <s:key name="delayed_artifacts_to_discard">
          <s:list/>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
```

```
</s:key>
<s:key name="eai:attributes">
  <s:dict>
    <s:key name="optionalFields">
      <s:list>
        <s:item>advertise_restart_required</s:item>
        <s:item>advertise_restart_required_reason</s:item>
        <s:item>alert_csv</s:item>
        <s:item>alert_csv_epoch</s:item>
        <s:item>artifacts_location_csv</s:item>
        <s:item>completed_summaries</s:item>
        <s:item>last_oaep</s:item>
        <s:item>last_osep</s:item>
        <s:item>partial_alert_delta</s:item>
        <s:item>partial_suppression_delta</s:item>
        <s:item>peer_load_stats_gla_15m</s:item>
        <s:item>peer_load_stats_gla_1m</s:item>
        <s:item>peer_load_stats_gla_5m</s:item>
        <s:item>peer_load_stats_max_runtime</s:item>
        <s:item>peer_load_stats_num_autosummary</s:item>
        <s:item>peer_load_stats_num_historical</s:item>
        <s:item>peer_load_stats_num_realtime</s:item>
        <s:item>peer_load_stats_num_running</s:item>
        <s:item>peer_load_stats_total_runtime</s:item>
        <s:item>peer_pid</s:item>
        <s:item>scheduler_disabled</s:item>
        <s:item>suppression_csv</s:item>
        <s:item>suppression_csv_epoch</s:item>
      </s:list>
    </s:key>
    <s:key name="requiredFields">
      <s:list>
        <s:item>last_artifact_log_entry_processed</s:item>
        <s:item>last_si_entry_processed</s:item>
        <s:item>mgmt_port</s:item>
        <s:item>peer_load_stats</s:item>
        <s:item>queue_blocked_count</s:item>
      </s:list>
    </s:key>
    <s:key name="wildcardFields">
      <s:list/>
    </s:key>
  </s:dict>
</s:key>
<s:key name="fixup_set">
  <s:list/>
</s:key>
<s:key name="host_port_pair">wimpy:13223</s:key>
<s:key name="is_captain">0</s:key>
<s:key name="kv_store_host_port">wimpy:18323</s:key>
<s:key name="label">wimpy-3</s:key>
<s:key name="last_heartbeat">1469221966</s:key>
<s:key name="mgmt_uri">https://wimpy:13223</s:key>
<s:key name="no_artifact_replications">0</s:key>
<s:key name="peer_scheme_host_port">https://wimpy:13223</s:key>
<s:key name="pending_job_count">0</s:key>
<s:key name="preferred_captain">1</s:key>
<s:key name="replication_count">0</s:key>
<s:key name="replication_port">12243</s:key>
<s:key name="replication_use_ssl">0</s:key>
<s:key name="site">default</s:key>
<s:key name="status">Up</s:key>
```

```
        <s:key name="status_counter">
          <s:dict>
            <s:key name="Complete">6</s:key>
            <s:key name="NonStreamingTarget">0</s:key>
            <s:key name="PendingDiscard">0</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/config

`https://<host>:<mPort>/services/shcluster/config`

List search head cluster node configuration.

GET

List search head cluster node configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
cxn_timeout	Low-level timeout, in seconds, for establishing connection between searchhead cluster nodes. Defaults to 60 seconds.
disabled	Indicates if this node is disabled.
heartbeat_period	Only valid for member nodes in a searchhead cluster. The time, in seconds, that a member attempts to send a heartbeat to the captain
heartbeat_timeout	Only valid for the captain node in a searchhead cluster configuration. The time, in seconds, before a captain considers a member down. Once a member is down, the captain initiates steps to replicate artifacts from the dead member to its live members. Defaults to 60 seconds.
id	Id of the SH cluster this member is a part of.
max_peer_rep_load	Maximum number of replications that can be ongoing as a target.
mode	Valid values: (disabled, member, captain, dynamic_captain) Defaults to disabled. Multiple values are permitted. Sets operational mode for this searchhead cluster node. Only one captain may exist per searchhead cluster.
percent_peers_to_restart	Percentage of peers to restart at the same time when doing a rolling restart.
ping_flag	For internal use to facilitate communication between the captain and members.

Name	Description
quiet_period	The time, in seconds, that a captain waits for members to add themselves to the searchhead cluster.
rcv_timeout	Low-level timeout, in seconds, for receiving data between searchhead cluster nodes. Defaults to 60 seconds.
register_replication_address	Valid only for nodes configured as members. The address on which a member is available for accepting replication data. This is useful in the cases where a member host machine has multiple interfaces and only one of them can be reached by another splunkd instance.
rep_cxn_timeout	Low-level timeout, in seconds, for establishing a connection for replicating data.
rep_max_rcv_timeout	Maximum cumulative time, in seconds, for receiving acknowledgement data from members. Defaults to 600s.
rep_max_send_timeout	Maximum time, in seconds, for sending replication slice data between searchhead cluster nodes. Defaults to 600s.
rep_rcv_timeout	Low-level timeout, in seconds, for receiving data between searchhead cluster nodes.
rep_send_timeout	Low-level timeout, in seconds, for sending replication data between searchhead cluster nodes. Defaults to 5 seconds.
replication_factor	Only valid for nodes configured as a captain. Determines how many copies of raw data are created in the searchhead cluster. This could be less than the number of searchhead cluster members. Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.
replication_port	TCP port to listen for replicated data from another searchhead cluster member.
replication_use_ssl	Indicates whether to use SSL when sending replication data.
restart_timeout	Only valid for nodes configured as a captain. The amount of time, in seconds, the captain waits for a member to come back when the member is restarted (to avoid the overhead of trying to fix the artifacts that were on the member). Defaults to 600 seconds. Note: This only works if the member is restarted from Splunk Web.
secret	Secret shared among the nodes in the searchhead cluster to prevent any arbitrary node from connecting to the searchhead cluster. If a member or searchhead is not configured with the same secret as the captain, it is not able to communicate with the captain. Corresponds to pass4SymmKey setting in `server.conf`.
send_timeout	Low-level timeout, in seconds, for sending data between searchhead cluster nodes. Defaults to 60 seconds.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/shcluster/config
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclusterconfig</title>
  <id>https://localhost:8089/services/shcluster/config</id>
  <updated>2014-10-15T08:50:47-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/config/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>config</title>
    <id>https://localhost:8089/services/shcluster/config/config</id>
    <updated>2014-10-15T08:50:47-07:00</updated>
    <link href="/services/shcluster/config/config" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/config/config" rel="list"/>
    <link href="/services/shcluster/config/config/_reload" rel="_reload"/>
    <link href="/services/shcluster/config/config" rel="edit"/>
    <link href="/services/shcluster/config/config/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="cxn_timeout">60</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="heartbeat_period">5</s:key>
        <s:key name="heartbeat_timeout">60</s:key>
        <s:key name="id">BB3116C0-73B9-459A-B473-254A18A69776</s:key>
        <s:key name="max_peer_rep_load">5</s:key>
        <s:key name="mode">dynamic_captain</s:key>
        <s:key name="percent_peers_to_restart">10</s:key>
        <s:key name="ping_flag">1</s:key>
        <s:key name="quiet_period">60</s:key>
        <s:key name="rcv_timeout">60</s:key>
        <s:key name="register_replication_address"></s:key>
        <s:key name="rep_cxn_timeout">60</s:key>
        <s:key name="rep_max_rcv_timeout">600</s:key>
        <s:key name="rep_max_send_timeout">600</s:key>
        <s:key name="rep_rcv_timeout">60</s:key>
        <s:key name="rep_send_timeout">60</s:key>
        <s:key name="replication_factor">2</s:key>
        <s:key name="replication_port">3456</s:key>
        <s:key name="replication_use_ssl">0</s:key>
        <s:key name="restart_timeout">60</s:key>
        <s:key name="secret">********</s:key>
        <s:key name="send_timeout">60</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/config/config

`https://<host>:<mPort>/services/shcluster/config/config`

Configure search head cluster members.

POST

Configure search head cluster members.

Request parameters

Name	Type	Description
rolling_restart	String	Sets the mode for search head cluster rolling restart. Options include: • `restart`: Initiates a rolling restart in classic mode (no guarantee of search continuity). • `searchable`: Initiates a rolling restart with minimum search interruption.
decommission_search_jobs_wait_secs	Integer	Specifies the amount of time, in seconds, that a search head cluster member waits for existing searches to complete before restarting. Default: 180 secs.
manual_detention	Use one of the following values: • **off**: Default. Remove the target search head from the detention state. • **on**: Put the target search head in manual detention mode.	Specifies whether to put the cluster member in manual detention.
target_uri	String	Specifies the target node you want to put in manual detention.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changed https://10.140.127.233:8089/services/shcluster/config/config -d
rolling_restart=searchable -d decommission_search_jobs_wait_secs=120
```

XML Response

```
http://docs.splunk.com/Documentation/Splunk/7.2.0/RESTREF/RESTcluster
```

Example request and response for manual detention of a cluster member

XML Request

```
curl -k -u admin:changedpwd https://fool01.sv.splunk.com:8095/services/shcluster/config/config -d
manual_detention=on -d target_uri=https://test.sv.splunk.com:8080
```

XML Response

```
<title>shclusterconfig</title>
  <id>https://10.140.127.233:8089/services/shcluster/config</id>
  <updated>2018-04-02T16:16:08-07:00</updated>
  <generator build="6a9fda63434" version="7.1.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/config/_reload" rel="_reload"/>
  <link href="/services/shcluster/config/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

shcluster/member/artifacts

`https://<host>:<mPort>/services/shcluster/member/artifacts`

Manage searchhead cluster member artifact configuration.

GET

List searchhead cluster members artifact configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

For each member:

Name	Description
status	Indicates the status of this artifact. Possible values are as follows. Complete The copy of this artifact contains the full complement of information. StreamingSource The copy of this artifact is sending data to member nodes for replication. StreamingTarget The copy of this artifact is receiving replicated data. NonStreamingTarget This copy of a warm artifact replication is in progress. Once replication is complete, the status changes to Complete. StreamingError The copy of this artifact encountered errors while streaming data. PendingTruncate The captain asked the member to truncate this copy of the artifact to a certain size and is waiting for confirmation. PendingDiscard The captain asked the member to discard this copy of the artifact and is waiting for confirmation. Standalone An artifact in the searchhead cluster that is not replicated.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/shcluster/member/artifacts
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustermemberartifacts</title>
  <id>https://localhost:8089/services/shcluster/member/artifacts</id>
  <updated>2014-10-15T08:51:46-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:51:46-07:00</updated>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="status">Complete</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:51:46-07:00</updated>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="remove"/>
```

```
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="status">Complete</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387900_290_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413387900_290_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:51:46-07:00</updated>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387900_290
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387900_290
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413387900_290
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="status">Complete</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413388200_291_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4_
_RMD5b9b800e209365567_at_1413388200_291_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:51:46-07:00</updated>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413388200_291
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413388200_291
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413388200_291
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="status">Complete</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/member/artifacts/{name}

`https://<host>:<mPort>/services/shcluster/member/artifacts/{name}`

Get `{name}` member artifact configuration.

GET

List `{name}` member artifact information.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
status	Indicates the status of this artifact. Possible values are as follows. Complete The copy of this artifact contains the full complement of information. StreamingSource The copy of this artifact is sending data to member nodes for replication. StreamingTarget The copy of this artifact is receiving replicated data. NonStreamingTarget This copy of a warm artifact replication is in progress. Once replication is complete, the status changes to Complete. StreamingError The copy of this artifact encountered errors while streaming data. PendingTruncate The captain asked the member to truncate this copy of the artifact to a certain size and is waiting for confirmation. PendingDiscard The captain asked the member to discard this copy of the artifact and is waiting for confirmation. Standalone An artifact in the searchhead cluster that is not replicated.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8189/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at
_1413518400_762_88888888-8888-8888-8888-888888888888
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
```

```
  <title>shclustermemberartifacts</title>
  <id>https://localhost:8089/services/shcluster/member/artifacts</id>
  <updated>2014-10-16T22:33:37-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888
-888888888888</title>
    <id>https://wimpy.splunk.com:55569/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4_
_RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-16T22:33:37-07:00</updated>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762
_88888888-8888-8888-8888-888888888888" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        ... eai:attributes node elided ...
        <s:key name="status">Complete</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/member/control/control/set_manual_detention

`https://<host>:<mPort>//services/shcluster/member/control/control/set_manual_detention`

Put the search head cluster member in manual detention mode or take the search head cluster member out of this mode. When a search head cluster member is in manual detention, it does not accept new search jobs, including both scheduled and ad-hoc searches. Existing search jobs run to completion. It also participates in cluster administration operations with the exception of artifact replication.

POST

Adjust search head manual detention mode.

Request parameters

Name	Type	Description
manual_detention	Use one of the following values.	Enable or disable manual detention.

Name	Type	Description
	• `off`: **Default**. Remove the search head from the detention state. • `on`: Put the search head in manual detention mode.	

Returned values

None

Example request and response

XML Request

```
curl  -u admin:password -k
https://localhost:8089/servicesNS/admin/search/shcluster/member/control/control/set_manual_detention -d
manual_detention=on
```

XML Response

```
 <title>shclustermembercontrol</title>
  <id>https://localhost:8089/servicesNS/admin/search/shcluster/member/control</id>
  <updated>2018-03-28T08:04:28-07:00</updated>
  <generator build="5fbc8cfc742f" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/shcluster/member/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

shcluster/member/consensus

`https://<host>:<mPort>/services/shcluster/member/consensus`
Get latest cluster configuration from the raft consensus protocol.

GET

Get latest cluster configuration from the raft consensus protocol.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

These values are returned for each member.

Name	Description
configuration_id	Unique id for this configuration.
servers_list	Comma-separated list of members that are part of the cluster. Each member is listed as scheme://host:port

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/shcluster/member/consensus
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustermemberconsensus</title>
  <id>https://localhost:8089/services/shcluster/member/consensus</id>
  <updated>2014-10-15T08:52:28-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>shc_cluster_configuration</title>
    <id>https://localhost:8089/services/shcluster/member/consensus/shc_cluster_configuration</id>
    <updated>2014-10-15T08:52:28-07:00</updated>
    <link href="/services/shcluster/member/consensus/shc_cluster_configuration" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/member/consensus/shc_cluster_configuration" rel="list"/>
    <link href="/services/shcluster/member/consensus/shc_cluster_configuration" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="configuration_id">4</s:key>
        ... eai:acl node elided ...
        <s:key name="servers_list">https://localhost:55560,https://localhost:55569</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/member/info

```
https://<host>:<mPort>/services/shcluster/member/info
```

Access searchhead cluster member node information.

GET

List member information.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

These values are returned for each member.

Name	Description
active_historical_search_count	Number of currently running historical searches.
active_realtime_search_count	Number of currently running realtime searches.
adhoc_searchhead	Flag that indicates if this member can run scheduled searches.
is_registered	Indicates if this member is registered with the searchhead cluster captain.
last_heartbeat_attempt	Timestamp for the last attempt to contact the captain.
maintenance_mode	N/A
peer_load_stats_gla_15m	Number of scheduled searches run in the last 15 minutes.
peer_load_stats_gla_1m	Number of scheduled searches run in the last one minute.
peer_load_stats_gla_5m	Number of scheduled searches run in the last five minutes.
peer_load_stats_max_runtime	N/A
peer_load_stats_num_autosummary	N/A
peer_load_stats_num_historical	N/A
peer_load_stats_num_realtime	N/A
peer_load_stats_num_running	N/A
peer_load_stats_total_runtime	N/A
restart_state	Indicates whether the member needs to be restarted to enable its searchhead cluster configuration.
status	Indicates the status of the member. Possible values are as follows. • Up • Pending • AutomaticDetention • ManualDetention • Restarting • ShuttingDown • ReassigningPrimaries • Decommissioning • GracefulShutdown • Down

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8189/services/shcluster/member/info
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustermemberinfo</title>
  <id>https://10.222.21.58:8089/services/shcluster/member/info</id>
  <updated>2018-03-29T12:05:35-07:00</updated>
  <generator build="d75793dbca24" version="7.1.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/member/info/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>member</title>
    <id>https://10.222.21.58:8089/services/shcluster/member/info/member</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/shcluster/member/info/member" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/member/info/member" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="active_historical_search_count">0</s:key>
        <s:key name="active_realtime_search_count">0</s:key>
        <s:key name="adhoc_searchhead">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="is_registered">1</s:key>
        <s:key name="last_heartbeat_attempt">1522350335</s:key>
        <s:key name="maintenance_mode">0</s:key>
        <s:key name="no_artifact_replications">0</s:key>
        <s:key name="peer_load_stats_gla_15m">0</s:key>
        <s:key name="peer_load_stats_gla_1m">0</s:key>
        <s:key name="peer_load_stats_gla_5m">0</s:key>
        <s:key name="peer_load_stats_max_runtime">0</s:key>
        <s:key name="peer_load_stats_num_autosummary">0</s:key>
        <s:key name="peer_load_stats_num_historical">0</s:key>
        <s:key name="peer_load_stats_num_realtime">0</s:key>
        <s:key name="peer_load_stats_num_running">0</s:key>
        <s:key name="peer_load_stats_total_runtime">0</s:key>
        <s:key name="restart_state">NoRestart</s:key>
        <s:key name="status">ManualDetention</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

shcluster/status

`https://<host>:<mPort>/services/shcluster/status`

Performs health checks to determine search head cluster health status, prior to a rolling upgrade or rolling restart.

Authentication and Authorization

Requires the `admin` role or `list_search_head_clustering` capability.

GET

Get search head cluster health status information .

Request parameters

Name	Type	Description
advanced	Boolean	Lists search head cluster status information in a verbose manner.

Returned values

These values are returned for each member.

Node	Name	Datatype	Description
Captain	*decommission_search_jobs_wait_secs*	Integer	Determines the maximum time, in seconds, that a member waits for search jobs to complete before it transitions to the down or GracefulShutdown state.
	dynamic_captain	Boolean	If true (1), then the captain is selected by elections. If false (0), then a static captain (no elections) is assigned.

Node	Name	Datatype	Description
	elected_captain	String	The time when new captain is elected.
	id	String	Specifies the search head cluster GUID.
	initialized_flag	Boolean	Indicates if the captain is initialized.
	label	String	Specifies the search head cluster label.
	max_failures_to_keep_majority	Boolean	Indicates how many more nodes can be down to keep majority.
	mgmt_uri	String	Specifies the URI and management port for the captain.
	min_peers_joined_flag	Boolean	*min_peers_joined_flag* is true when there are at least as many search head peers as the replication_factor.
	rolling_restart	String	Shows the restart mode, either restart or searchable.
	rolling_restart_flag	Boolean	*rolling_restart_flag* is true when a rolling restart is in progress.
	rolling_upgrade_flag	Boolean	*rolling_upgrade_flag* is true when a rolling upgrade is in progress.
	service_ready_flag	Boolean	*service_ready_flag* is true when everything is up and running as expected and "ready to go!"
	stable_captain	Boolean	Indicates stable captain based on heartbeat.
Member	*label*	String	Specifies the search head label.
	last_conf_replication	String	Specifies when the member last pulled a set of configurations from the captain.
	manual_detention	String	Indicates if the member is in manual detention. Use *off* or *on*.
	mgmt_uri	String	Specifies the URI and management port for the member.
	mgmt_uri_alias	String	Specifies the URI and management port for the member.
	out_of_sync_node	Boolean	*out_of_sync_node* is true when the member is out of sync.
	preferred_captain	Boolean	Indicates the member's preference for captaincy.
	restart_required	Boolean	*restart_required* is true when member requests a restart
	splunk_version	String	Splunk version running on the search head.
	status	String	Indicates the current status of the member.

Example request and response

XML Request

```
curl -k -u admin:changed123 https://localhost:8089/services/shcluster/status?advanced=1?
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclusterstatus</title>
  <id>https://10.222.21.58:8089/services/shcluster/status</id>
  <updated>2018-03-29T12:00:50-07:00</updated>
  <generator build="d75793dbca24" version="7.1.0"/>
```

```
<author>
  <name>Splunk</name>
</author>
<link href="/services/shcluster/status/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>status</title>
  <id>https://10.222.21.58:8089/services/shcluster/status/status</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/shcluster/status/status" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/shcluster/status/status" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="captain">
        <s:dict>
          <s:key name="dynamic_captain">1</s:key>
          <s:key name="elected_captain">Thu Mar 29 11:58:04 2018</s:key>
          <s:key name="id">93E0DBE8-A435-462F-BF7D-6297C9D9F939</s:key>
          <s:key name="initialized_flag">1</s:key>
          <s:key name="label">ip-10-222-21-58</s:key>
          <s:key name="mgmt_uri">https://10.222.21.58:8089</s:key>
          <s:key name="min_peers_joined_flag">1</s:key>
          <s:key name="rolling_restart_flag">0</s:key>
          <s:key name="service_ready_flag">1</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="peers">
        <s:dict>
          <s:key name="2EF65F8B-2689-4A77-B056-E824B2FEB0CA">
```

```
       <s:dict>
        <s:key name="label">ip-10-222-25-57</s:key>
        <s:key name="last_conf_replication">Thu Mar 29 12:00:49 2018</s:key>
        <s:key name="mgmt_uri">https://10.222.25.57:8089</s:key>
        <s:key name="mgmt_uri_alias">https://10.222.25.57:8089</s:key>
        <s:key name="status">Up</s:key>
       </s:dict>
      </s:key>
      <s:key name="48E93CC7-9A2D-40BE-BAF5-EB9C87200FA5">
       <s:dict>
        <s:key name="label">ip-10-222-31-70</s:key>
        <s:key name="last_conf_replication">Thu Mar 29 12:00:46 2018</s:key>
        <s:key name="mgmt_uri">https://10.222.31.70:8089</s:key>
        <s:key name="mgmt_uri_alias">https://10.222.31.70:8089</s:key>
        <s:key name="status">Up</s:key>
       </s:dict>
      </s:key>
      <s:key name="F8AB4ECE-F14A-415E-AEBE-9BC87216D056">
       <s:dict>
        <s:key name="label">ip-10-222-21-58</s:key>
        <s:key name="mgmt_uri">https://10.222.21.58:8089</s:key>
        <s:key name="mgmt_uri_alias">https://10.222.21.58:8089</s:key>
        <s:key name="status">Up</s:key>
       </s:dict>
      </s:key>
     </s:dict>
    </s:key>
   </s:dict>
  </content>
 </entry>
</feed>
```

upgrade/shc/recovery

`https://<host>:<mPort>/services/upgrade/shc/recovery`

Return search head cluster to ready state after automated rolling upgrade failure.

Authentication and Authorization

Requires admin role or another role containing these capabilties:

- upgrade_splunk_shc
- list_search_head_clustering
- list_settings
- use_remote_proxy

POST

Return SHC to ready state after automated rolling upgrade failure.

Request parameters

None

Returned values

Name	Type	Description
status	String	Status of HTTP request. For example, "succeeded" or "failed"

Example request and response

JSON Request

```
curl -X POST -u admin:pass -k https://localhost:8089/services/upgrade/shc/recovery?output_mode=json
```

JSON Response

```
{
    "updated":"2022-11-24T17:36:20+0000",
    "author":"Splunk",
    "layout":"props",
    "entry":[
        {
            "title":"recovery",
            "id":"/services/upgrade/shc/recovery",
            "updated":"2022-11-24T17:36:20+0000",
            "links":{
                "alternate":{
                    "href":"shc/recovery"
                }
            },
            "content":{
                "message":"Instance recovered successfully",
                "status":"succeeded"
            }
        }
    ]
}
```

upgrade/shc/status

```
https://<host>:<mPort>/services/upgrade/shc/status
```

Check the status of an automated search head cluster rolling upgrade.

Authentication and Authorization

Requires admin role or another role containing these capabilities:

- upgrade_splunk_shc
- list_search_head_clustering
- list_settings
- use_remote_proxy

GET

Check the status of automated SHC rolling upgrade.

Request parameters

None

Returned values

Name	Type	Description
upgrade status	String	Status of automated rollling upgrade for entire clutser.
peers_to_upgrade	Number	The total number of cluster members to upgrade.
overall_peers_upgraded	Number	The number of cluster members upgraded at present.
overall_peers_upgraded_percentage	Number	The percentage of total cluster members upgraded at present.
name	String	The name of the individual cluster member.
status	String	Upgrade status of the individual cluster member.
last_modified	String	Date and time the individual cluster member was modified.

Example request and response

JSON Request

```
curl -u admin:pass -k https://localhost:8089/services/upgrade/shc/status?output_mode=json
```

JSON Response

```
{
    "updated":"2022-11-24T17:33:28+0000",
    "author":"Splunk",
    "layout":"props",
    "entry":[
        {
            "title":"status",
            "id":"/services/upgrade/shc/status",
            "updated":"2022-11-24T17:33:28+0000",
            "links":{
                "alternate":{
                    "href":"shc/status"
                }
            },
            "content":{
                "message":{
                    "upgrade_status":"completed",
                    "statistics":{
                        "peers_to_upgrade":3,
                        "overall_peers_upgraded":3,
                        "overall_peers_upgraded_percentage":100
                    },
                    "peers":[
                        {
                            "name":"sh2",
                            "status":"upgraded",
                            "last_modified":"Thu Nov 24 17:29:41 2022"
                        },
                        {
                            "name":"sh1",
                            "status":"upgraded",
                            "last_modified":"Thu Nov 24 17:28:07 2022"
                        },
                        {
                            "name":"sh3",
                            "status":"upgraded",
                            "last_modified":"Thu Nov 24 17:31:15 2022"
                        }
                    ]
                }
            }
        }
    ]
}
```

upgrade/shc/upgrade

`https://<host>:<mPort>/services/upgrade/shc/upgrade`

Initiate an automated rolling upgrade of a search head cluster.

Authentication and Authorization

Requires admin role or another role containing these capabilities:

- upgrade_splunk_shc
- list_search_head_clustering
- list_settings
- use_remote_proxy

POST

Initiate automated SHC rolling upgrade.

Request parameters

None

Returned values

Name	Type	Description
status	String	Status of HTTP request. For example, "succeeded" or "failed".

Example request and response

JSON Request

```
curl -X POST -u admin:pass -k https://localhost:8089/services/upgrade/shc/upgrade?output_mode=json
```

JSON Response

```
{
    "updated":"2022-11-24T17:25:54+0000",
    "author":"Splunk",
    "layout":"props",
    "entry":[
        {
            "title":"upgrade",
            "id":"/services/upgrade/shc/upgrade",
            "updated":"2022-11-24T17:25:54+0000",
            "links":{
                "alternate":{
                    "href":"shc/upgrade"
                }
            },
            "content":{
                "message":"Upgrade initiated",
                "status":"succeeded"
            }
        }
    ]
}
```

Configuration endpoints

Configuration endpoint descriptions

Manage configuration files and settings.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Additional configuration file information

For details about working with configuration files, see the following topics in the *Admin Manual*.

- About configuration files
- Configuration file precedence

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. Configuration endpoints are generally not accessible in Splunk Cloud Platform.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

---

configs/conf-{file}

```
https://<host>:<mPort>/services/configs/conf-{file}
```

Access and update a `.conf` configuration file.

For additional information, see the following resources.

- properties/{file}

GET

List `{file}` configuration file stanzas.

Namespace determines which instance of the file is retrieved.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/configs/conf-props
```

XML Response

```
.
.
.
 <title>conf-props</title>
 <id>https://localhost:8089/services/configs/conf-props</id>
 <updated>2011-07-08T01:01:26-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/configs/conf-props/_new" rel="create"/>
 <link href="/services/configs/conf-props/_reload" rel="_reload"/>
 <!-- opensearch nodes elided for brevity. -->
 <s:messages/>
 <entry>
   <title>(?i)source::....zip(.\d+)?</title>
   <id>https://localhost:8089/servicesNS/nobody/system/configs/conf-props
/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F</id>
   <updated>2011-07-08T01:01:26-07:00</updated>
   <link href="/servicesNS/nobody/system/configs/conf-props/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F"
rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/configs/conf-props/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F"
rel="list"/>
   <link
href="/servicesNS/nobody/system/configs/conf-props/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/system/configs/conf-props/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F"
rel="edit"/>
   <link
href="/servicesNS/nobody/system/configs/conf-props/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F/disable"
```

```
rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="ANNOTATE_PUNCT">1</s:key>
       <s:key name="BREAK_ONLY_BEFORE"/>
       <s:key name="BREAK_ONLY_BEFORE_DATE">1</s:key>
       <s:key name="CHARSET">UTF-8</s:key>
       <s:key name="DATETIME_CONFIG">/etc/datetime.xml</s:key>
       <s:key name="HEADER_MODE"/>
       <s:key name="LEARN_SOURCETYPE">1</s:key>
       <s:key name="LINE_BREAKER_LOOKBEHIND">100</s:key>
       <s:key name="MAX_DAYS_AGO">2000</s:key>
       <s:key name="MAX_DAYS_HENCE">2</s:key>
       <s:key name="MAX_DIFF_SECS_AGO">3600</s:key>
       <s:key name="MAX_DIFF_SECS_HENCE">604800</s:key>
       <s:key name="MAX_EVENTS">256</s:key>
       <s:key name="MAX_TIMESTAMP_LOOKAHEAD">128</s:key>
       <s:key name="MUST_BREAK_AFTER"/>
       <s:key name="MUST_NOT_BREAK_AFTER"/>
       <s:key name="MUST_NOT_BREAK_BEFORE"/>
       <s:key name="NO_BINARY_CHECK">1</s:key>
       <s:key name="SEGMENTATION">indexing</s:key>
       <s:key name="SEGMENTATION-all">full</s:key>
       <s:key name="SEGMENTATION-inner">inner</s:key>
       <s:key name="SEGMENTATION-outer">outer</s:key>
       <s:key name="SEGMENTATION-raw">none</s:key>
       <s:key name="SEGMENTATION-standard">standard</s:key>
       <s:key name="SHOULD_LINEMERGE">1</s:key>
       <s:key name="TRANSFORMS"/>
       <s:key name="TRUNCATE">10000</s:key>
       <s:key name="disabled">0</s:key>
       <!-- eai:acl nodes elided for brevity. -->
       <s:key name="eai:appName">search</s:key>
       <s:key name="eai:userName">admin</s:key>
       <s:key name="maxDist">100</s:key>
       <s:key name="sourcetype">preprocess-zip</s:key>
       <s:key name="unarchive_cmd">_auto</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Add stanza to `{file}` configuration file.

Namespace determines which instance of the file is updated.

Authorization

Requires `admin_all_objects` capability.

Request parameters

Name	Type	Description
name	String	**Required**. Stanza name in `{file}` configuration file.
<variable>	String	Arbritrary number of key/value pairs.

Name	Type	Description

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/configs/conf-props -d name=myblog
```

XML Response

```
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>conf-props</title>
  <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props</id>
  <updated>2015-07-17T10:50:13+08:00</updated>
  <generator build="ab1a3707c875" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/configs/conf-props/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/configs/conf-props/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/configs/conf-props/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>myblog</title>
    <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myblog</id>
    <updated>2015-07-17T10:50:13+08:00</updated>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog" rel="list"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog" rel="edit"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog" rel="remove"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog/move" rel="move"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="ANNOTATE_PUNCT">1</s:key>
        <s:key name="AUTO_KV_JSON">1</s:key>
        <s:key name="BREAK_ONLY_BEFORE"></s:key>
        <s:key name="BREAK_ONLY_BEFORE_DATE">1</s:key>
        <s:key name="CHARSET">UTF-8</s:key>
        <s:key name="DATETIME_CONFIG">/etc/datetime.xml</s:key>
        <s:key name="HEADER_MODE"></s:key>
        <s:key name="LEARN_SOURCETYPE">1</s:key>
        <s:key name="LINE_BREAKER_LOOKBEHIND">100</s:key>
        <s:key name="MAX_DAYS_AGO">2000</s:key>
        <s:key name="MAX_DAYS_HENCE">2</s:key>
        <s:key name="MAX_DIFF_SECS_AGO">3600</s:key>
        <s:key name="MAX_DIFF_SECS_HENCE">604800</s:key>
        <s:key name="MAX_EVENTS">256</s:key>
        <s:key name="MAX_TIMESTAMP_LOOKAHEAD">128</s:key>
        <s:key name="MUST_BREAK_AFTER"></s:key>
        <s:key name="MUST_NOT_BREAK_AFTER"></s:key>
        <s:key name="MUST_NOT_BREAK_BEFORE"></s:key>
        <s:key name="SEGMENTATION">indexing</s:key>
        <s:key name="SEGMENTATION-all">full</s:key>
        <s:key name="SEGMENTATION-inner">inner</s:key>
        <s:key name="SEGMENTATION-outer">outer</s:key>
        <s:key name="SEGMENTATION-raw">none</s:key>
        <s:key name="SEGMENTATION-standard">standard</s:key>
        <s:key name="SHOULD_LINEMERGE">1</s:key>
        <s:key name="TRANSFORMS"></s:key>
        <s:key name="TRUNCATE">10000</s:key>
        <s:key name="detect_trailing_nulls">0</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>power</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">global</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="maxDist">100</s:key>
        <s:key name="priority"></s:key>
        <s:key name="sourcetype"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

configs/conf-{file}/{stanza}

```
https://<host>:<mPort>/services/configs/conf-{file}/{stanza}
```

Manage configuration file stanzas.

DELETE

Delete `{stanza}` in `{file}` configuration file.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myweblogs
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"

     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
 <title>conf-props</title>
 <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props</id>
 <updated>2011-07-08T01:01:27-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/search/configs/conf-props/_new" rel="create"/>
 <link href="/servicesNS/nobody/search/configs/conf-props/_reload" rel="_reload"/>
 <!-- opensearch nodes elided for brevity. -->
 <s:messages/>
</feed>
```

GET

Get `{stanza}` in `{file}` configuration file.

Request parameters
None

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message
```

XML Response

```
.
.
.
 <title>conf-eventtypes</title>
 <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-eventtypes</id>
 <updated>2014-07-01T13:08:45-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/search/configs/conf-eventtypes/_new" rel="create"/>
 <link href="/servicesNS/nobody/search/configs/conf-eventtypes/_reload" rel="_reload"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>splunkd_message</title>
   <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message</id>
   <updated>2014-07-01T13:08:45-07:00</updated>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message" rel="alternate"/>
   <author>
     <name>admin</name>
   </author>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message" rel="list"/>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message" rel="edit"/>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message" rel="remove"/>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message/move" rel="move"/>
   <link href="/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="CHARSET">UTF-8</s:key>
       <s:key name="description"></s:key>
       <s:key name="disabled">0</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">search</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">admin</s:key>
```

```
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">global</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list/>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list>
              <s:item>.*</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="priority">1</s:key>
      <s:key name="search"></s:key>
      <s:key name="tags"></s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update or add property to `{stanza}` in `{file}` configuration file.

Request parameters

Name	Type	Description
<variable>	String	Arbitrary number of key/value pairs to update.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myweblogs -d
SHOULD_LINEMERGE=true
```

XML Response

```
.
.
.
 <title>conf-props</title>
 <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props</id>
 <updated>2011-07-08T01:01:26-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/search/configs/conf-props/_new" rel="create"/>
 <link href="/servicesNS/nobody/search/configs/conf-props/_reload" rel="_reload"/>
 <!-- opensearch nodes elided for brevity. -->
 <s:messages/>
 <entry>
   <title>myweblogs</title>
   <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myweblogs</id>
   <updated>2011-07-08T01:01:26-07:00</updated>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs" rel="alternate"/>
   <author>
     <name>admin</name>
   </author>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs" rel="list"/>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs" rel="edit"/>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs" rel="remove"/>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs/move" rel="move"/>
   <link href="/servicesNS/nobody/search/configs/conf-props/myweblogs/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="ANNOTATE_PUNCT">1</s:key>
       <s:key name="BREAK_ONLY_BEFORE"/>
       <s:key name="BREAK_ONLY_BEFORE_DATE">1</s:key>
       <s:key name="CHARSET">UTF-8</s:key>
       <s:key name="DATETIME_CONFIG">/etc/datetime.xml</s:key>
       <s:key name="HEADER_MODE"/>
       <s:key name="LEARN_SOURCETYPE">1</s:key>
       <s:key name="LINE_BREAKER_LOOKBEHIND">100</s:key>
       <s:key name="MAX_DAYS_AGO">2000</s:key>
       <s:key name="MAX_DAYS_HENCE">2</s:key>
       <s:key name="MAX_DIFF_SECS_AGO">3600</s:key>
       <s:key name="MAX_DIFF_SECS_HENCE">604800</s:key>
       <s:key name="MAX_EVENTS">256</s:key>
       <s:key name="MAX_TIMESTAMP_LOOKAHEAD">128</s:key>
       <s:key name="MUST_BREAK_AFTER"/>
       <s:key name="MUST_NOT_BREAK_AFTER"/>
       <s:key name="MUST_NOT_BREAK_BEFORE"/>
       <s:key name="SEGMENTATION">indexing</s:key>
       <s:key name="SEGMENTATION-all">full</s:key>
       <s:key name="SEGMENTATION-inner">inner</s:key>
       <s:key name="SEGMENTATION-outer">outer</s:key>
       <s:key name="SEGMENTATION-raw">none</s:key>
       <s:key name="SEGMENTATION-standard">standard</s:key>
       <s:key name="SHOULD_LINEMERGE">1</s:key>
       <s:key name="TRANSFORMS"/>
       <s:key name="TRUNCATE">10000</s:key>
       <s:key name="disabled">0</s:key>
       <!-- eai:acl nodes elided for brevity. -->
       <s:key name="eai:appName">search</s:key>
       <s:key name="eai:userName">admin</s:key>
       <s:key name="maxDist">100</s:key>
     </s:dict>
   </content>
 </entry>
```

properties

```
https://<host>:<mPort>/services/properties
```

Manage `.conf` configuration files.

GET

List all system and app configuration files.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties
```

XML Response

```
.
.
.
 <title>properties</title>
 <id>https://localhost:8089/services/properties</id>
 <updated>2014-07-01T13:17:36-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <entry>
   <title>alert_actions</title>
   <id>https://localhost:8089/services/properties/alert_actions</id>
   <updated>2014-07-01T13:17:36-07:00</updated>
   <link href="/services/properties/alert_actions" rel="alternate"/>
 </entry>
```

```
<entry>
  <title>app</title>
  <id>https://localhost:8089/services/properties/app</id>
  <updated>2014-07-01T13:17:36-07:00</updated>
  <link href="/services/properties/app" rel="alternate"/>
</entry>
<entry>
  <title>audit</title>
  <id>https://localhost:8089/services/properties/audit</id>
  <updated>2014-07-01T13:17:36-07:00</updated>
  <link href="/services/properties/audit" rel="alternate"/>
</entry>
      .
      .
      .
    elided
      .
      .
      .
<entry>
  <title>viewstates</title>
  <id>https://localhost:8089/services/properties/viewstates</id>
  <updated>2014-07-01T13:17:36-07:00</updated>
  <link href="/services/properties/viewstates" rel="alternate"/>
</entry>
<entry>
  <title>web</title>
  <id>https://localhost:8089/services/properties/web</id>
  <updated>2014-07-01T13:17:36-07:00</updated>
  <link href="/services/properties/web" rel="alternate"/>
</entry>
<entry>
  <title>workflow_actions</title>
  <id>https://localhost:8089/services/properties/workflow_actions</id>
  <updated>2014-07-01T13:17:36-07:00</updated>
  <link href="/services/properties/workflow_actions" rel="alternate"/>
</entry>
```

POST

Create a configuration file.

Usage details

The namespace specified in the URL determines where the configuration file is created. For example, `/services/properties` creates the file in the `$SPLUNK_BASE/etc/system/local` directory and `servicesNS/nobody/search` creates the file in the `$SPLUNK_BASE/etc/apps/search/local` directory.

Authentication and Authorization

Requires the `admin_all_objects` capability.

Request parameters

Name	Type	Description
__conf	String	**Required**. Name of the configuration file to create. (Note double underscore prefix.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties -d __conf=myAppConfigFile
```

XML Response

No response body.

Returns: `HTTP status = 201 (created)`

---

properties/{file}

```
https://<host>:<mPort>/services/properties/{file}
```

Access stanzas in specified configuration file.

Usage details

The URL namespace determines the scope of visible stanzas. The endpoint returns all stanzas of the specified configuration file, for all configuration files and stanzas visible in the namespace.

GET

List stanzas in `{file}` configuration file.

Request parameters

None

Response keys

This endpoint returns an `<entry>` for each stanza in addition to `<default>` stanzas.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/properties/eventtypes
```

XML Response

```
.
.
```

```
.
 <title>eventtypes</title>
 <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes</id>
 <updated>2014-07-17T10:24:53-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <entry>
   <title>default</title>
   <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes/default</id>
   <updated>2014-07-17T10:24:53-07:00</updated>
   <link href="/servicesNS/nobody/search/properties/eventtypes/default" rel="alternate"/>
 </entry>
 <entry>
   <title>internal_search_terms</title>
   <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes/internal_search_terms</id>
   <updated>2014-07-17T10:24:53-07:00</updated>
   <link href="/servicesNS/nobody/search/properties/eventtypes/internal_search_terms" rel="alternate"/>
 </entry>
 <entry>
   <title>proxylogs</title>
   <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes/proxylogs</id>
   <updated>2014-07-17T10:24:53-07:00</updated>
   <link href="/servicesNS/nobody/search/properties/eventtypes/proxylogs" rel="alternate"/>
 </entry>
 <entry>
   <title>splunkd-access</title>
   <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes/splunkd-access</id>
   <updated>2014-07-17T10:24:53-07:00</updated>
   <link href="/servicesNS/nobody/search/properties/eventtypes/splunkd-access" rel="alternate"/>
 </entry>
 <entry>
   <title>splunkd-log</title>
   <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes/splunkd-log</id>
   <updated>2014-07-17T10:24:53-07:00</updated>
   <link href="/servicesNS/nobody/search/properties/eventtypes/splunkd-log" rel="alternate"/>
 </entry>
 <entry>
   <title>splunkd_message</title>
   <id>https://localhost:8089/servicesNS/nobody/search/properties/eventtypes/splunkd_message</id>
   <updated>2014-07-17T10:24:53-07:00</updated>
   <link href="/servicesNS/nobody/search/properties/eventtypes/splunkd_message" rel="alternate"/>
 </entry>
</feed>
```

POST

Add stanza to `{file}` configuration file.

Request parameters

Name	Type	Description
__stanza	String	**Required**. The key/value pair of the stanza to add. Note double underscore prefix.

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/properties/eventtypes -d
__stanza=proxylogs
```

XML Response

No data returned in body.

Returns: `HTTP status 201 (created)`

---

properties/{file}/{stanza}

```
https://<host>:<mPort>/services/properties/{file}/{stanza}
```

Access and update key/value pair(s) of the specified configuration file and stanza.

GET

List `{stanza}` key/value pair(s) of `{file}` configuration file.

Usage details
The URL namespace determines the scope of visible stanzas. This endpoint returns all stanzas of the specified configuration file for all configuration files and stanzas visible in the namespace.

Request parameters
None

Response keys
Each `<entry>` is a `{stanza}` key with a `<content>` value.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs
```

XML Response

```
.
.
```

```
.
 <title>proxylogs</title>
 <id>https://localhost:8089/services/properties/props/proxylogs</id>
 <updated>2011-07-08T12:08:52-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <entry>
   <title>ANNOTATE_PUNCT</title>
   <id>https://localhost:8089/services/properties/props/proxylogs/ANNOTATE_PUNCT</id>
   <updated>2011-07-08T12:08:52-07:00</updated>
   <link href="/services/properties/props/proxylogs/ANNOTATE_PUNCT" rel="alternate"/>
   <content type="text">True</content>
 </entry>
 <entry>
   <title>BREAK_ONLY_BEFORE</title>
   <id>https://localhost:8089/services/properties/props/proxylogs/BREAK_ONLY_BEFORE</id>
   <updated>2011-07-08T12:08:52-07:00</updated>
   <link href="/services/properties/props/proxylogs/BREAK_ONLY_BEFORE" rel="alternate"/>
   <content type="text"/>
 </entry>
 <entry>
   <title>BREAK_ONLY_BEFORE_DATE</title>
   <id>https://localhost:8089/services/properties/props/proxylogs/BREAK_ONLY_BEFORE_DATE</id>
   <updated>2011-07-08T12:08:52-07:00</updated>
   <link href="/services/properties/props/proxylogs/BREAK_ONLY_BEFORE_DATE" rel="alternate"/>
   <content type="text">True</content>
 </entry>
       .
       .
       .
     elided
       .
       .
       .
 <entry>
   <title>TRANSFORMS</title>
   <id>https://localhost:8089/services/properties/props/proxylogs/TRANSFORMS</id>
   <updated>2011-07-08T12:08:52-07:00</updated>
   <link href="/services/properties/props/proxylogs/TRANSFORMS" rel="alternate"/>
   <content type="text"/>
 </entry>
 <entry>
   <title>TRUNCATE</title>
   <id>https://localhost:8089/services/properties/props/proxylogs/TRUNCATE</id>
   <updated>2011-07-08T12:08:52-07:00</updated>
   <link href="/services/properties/props/proxylogs/TRUNCATE" rel="alternate"/>
   <content type="text">10000</content>
 </entry>
 <entry>
   <title>maxDist</title>
   <id>https://localhost:8089/services/properties/props/proxylogs/maxDist</id>
   <updated>2011-07-08T12:08:52-07:00</updated>
   <link href="/services/properties/props/proxylogs/maxDist" rel="alternate"/>
   <content type="text">100</content>
 </entry>
```

POST

Add or update one or more key/value pair(s) in `{stanza}` of `{file}` configuration file.

Request parameters

Name	Type	Description
<variable>	String	**Required**. One or more key/value pair(s).

Response keys

A response `<message>` indicates update success or failure.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs -d NO_BINARY_CHECK=true -d
CHARSET=UTF-8
```

XML Response

```
<response>
 <messages>
   <msg type="INFO">Successfully modified 2 key(s)</msg>
 </messages>
</response>
```

properties/{file}/{stanza}/{key}

```
https://<host>:<mPort>/services/properties/{file}/{stanza}/{key}
```

Access and update values for the specified configuration file, stanza, and key.

GET

Get a plaintext `{key}` value for a configuration file stanza and key.

Request parameters

None

Response keys

Name	Description
<variable>	Plaintext value.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs/SHOULD_LINEMERGE
```

XML Response

```
True
```

POST

Update a plaintext `{key}` value for a configuration file stanza and key.

Request parameters

Name	Type	Description
<variable>	String	**Required**. Plaintext value.

Response keys

Message indicates update success or failure.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs/SHOULD_LINEMERGE -d
value=false
```

XML Response

```
<response>
 <messages>
   <msg type="INFO">Successfully modified 1 key(s)</msg>
 </messages>
</response>
```

Deployment endpoints

Deployment endpoint descriptions

Manage deployment servers and clients.

A deployment server configures a deployment client. Deployment clients and servers can reside on separate, distributed, Splunk instances or can reside on the same instance.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. Deployment endpoints are generally not accessible in Splunk Cloud Platform.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

---

deployment/client

`https://<host>:<mPort>/services/deployment/client`

List deployment client configuration and status.

GET

Get deployment client list with enabled status, server class, and host and port number of each.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

For each deployment client, the following values are returned.

Name	Description
disabled	Disabled status: `0` = Enabled `1` = Disabled
serverClasses	List of member server classes for app download authorization.
targetUri	Host and port number (*<host>:<port>*).

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/client
```

XML Response

```
...
 <title>deploymentclient</title>
 <id>https://localhost:8089/services/deployment/client</id>
 <updated>2011-07-11T00:35:37-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>deployment-client</title>
   <id>https://localhost:8089/services/deployment/client/deployment-client</id>
   <updated>2011-07-11T00:35:37-07:00</updated>
   <link href="/services/deployment/client/deployment-client" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/client/deployment-client" rel="list"/>
   <link href="/services/deployment/client/deployment-client" rel="edit"/>
   <link href="/services/deployment/client/deployment-client/reload" rel="reload"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">0</s:key>
       ... eai:acl node elided ...
       <s:key name="serverClasses">
```

```
         <s:list>
           <s:item>dstest:dstestapp</s:item>
         </s:list>
       </s:key>
       <s:key name="targetUri">essplunk:8089</s:key>
     </s:dict>
   </content>
 </entry>
```

deployment/client/config

`https://<host>:<mPort>/services/deployment/client/config`

Get deployment client configuration and status.

GET

Get deployment client enabled status, server class for app distribution, and host and port number.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
disabled	Disabled status: `0` = Enabled `1` = Disabled
serverClasses	List of member server classes for app download authorization.
targetUri	Host and port number (*`<host>:<port>`*).

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/client/config
```

XML Response

```
 <title>deploymentclient</title>
 <id>https://localhost:8089/services/deployment/client</id>
 <updated>2013-07-31T20:49:58-07:00</updated>
 <generator build="172889" version="6.0"/>
```

```
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/client/listIsDisabled" rel="listIsDisabled"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>config</title>
  <id>https://localhost:8089/services/deployment/client/config</id>
  <updated>2013-07-31T20:49:58-07:00</updated>
  <link href="/services/deployment/client/config" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/deployment/client/config" rel="list"/>
  <link href="/services/deployment/client/config" rel="edit"/>
  <link href="/services/deployment/client/config/reload" rel="reload"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      ... eai:acl node elided ...
      ... eai:attributes node elided ...
      <s:key name="serverClasses">
        <s:list>
          <s:item>sc_apps_wma:wma-app2</s:item>
          <s:item>sc_apps_wma:wma-app1</s:item>
          <s:item>sc_mach_type:wma-app2</s:item>
          <s:item>sc_new:wma-app2</s:item>
          <s:item>sc_new:wma-app1</s:item>
        </s:list>
      </s:key>
      <s:key name="targetUri">localhost:8089</s:key>
    </s:dict>
  </content>
</entry>
```

deployment/client/config/listIsDisabled

`https://<host>:<mPort>/services/deployment/client/config/listIsDisabled`

Get deployment client status.

GET

Get deployment client disabled status.

Request parameters

None

Returned values

Name	Description

Name	Description
disabled	Disabled status: 0 = Enabled 1 = Disabled

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/client/config/listIsDisabled
```

XML Response

```
...
 <title>deploymentclient</title>
 <id>https://localhost:8089/services/deployment/client</id>
 <updated>2013-08-04T18:49:25-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/client/listIsDisabled" rel="listIsDisabled"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>default</title>
   <id>https://localhost:8089/services/deployment/client/default</id>
   <updated>2013-08-04T18:49:25-07:00</updated>
   <link href="/services/deployment/client/default" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/client/default" rel="list"/>
   <link href="/services/deployment/client/default" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">0</s:key>
       ... eai:acl node elided ...
     </s:dict>
   </content>
 </entry>
```

deployment/client/config/reload

Access information on reloading the named client.

POST

Access client reload information.

Request parameters
No parameters for this request.

Returned values

Status Code	Description
200	Endpoint returned successfully.
400	Request error. See response body for details.
401	Authentication failure: must pass valid credentials with request.
403	Insufficient permissions to access resource.
404	Specified resoruce does not exist.
409	Request error: this operation is invalid for this item. See response body for details.
500	Internal server error. See response body for details.

Example request and response

XML Request

```
curl -k -u admin:pass -X POST https://localhost:8089/services/deployment/client/config/reload
```

XML Response

```
...
 <title>deploymentclient</title>
 <id>https://localhost:8089/services/deployment/client</id>
 <updated>2013-10-07T15:49:06-07:00</updated>
 <generator build="182462" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/client/listIsDisabled" rel="listIsDisabled"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>config</title>
   <id>https://localhost:8089/services/deployment/client/config</id>
   <updated>2013-10-07T15:49:06-07:00</updated>
   <link href="/services/deployment/client/config" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/client/config" rel="list"/>
   <link href="/services/deployment/client/config" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">1</s:key>
       ... eai:acl node elided ...
```

```
    </s:dict>
  </content>
</entry>
```

deployment/client/{name}/reload

`https://<host>:<mPort>/services/deployment/client/{name}/reload`
Restart and reload the `{name}` deployment client.

POST

Restart and reload `{name}` deployment client.

Request parameters

None

Returned values

Name	Description
disabled	Disabled status: `0` = Enabled `1` = Disabled
serverClasses	List of member server classes for app download authorization.
targetUri	Host and port number (*`<host>:<port>`*).

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/client/deployment-client/reload
```

XML Response

```
...
 <title>deploymentclient</title>
 <id>https://localhost:8089/services/deployment/client</id>
 <updated>2011-07-11T00:39:23-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>deployment-client</title>
   <id>https://localhost:8089/services/deployment/client/deployment-client</id>
```

```
  <updated>2011-07-11T00:39:23-07:00</updated>
  <link href="/services/deployment/client/deployment-client" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/deployment/client/deployment-client" rel="list"/>
  <link href="/services/deployment/client/deployment-client" rel="edit"/>
  <link href="/services/deployment/client/deployment-client/reload" rel="reload"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      ... eai:acl node elided ...
      <s:key name="serverClasses">
        <s:list>
          <s:item>dstest:dstestapp</s:item>
        </s:list>
      </s:key>
      <s:key name="targetUri">tiny:8089</s:key>
    </s:dict>
  </content>
</entry>
```

deployment/server/applications

`https://<host>:<mPort>/services/deployment/server/applications`

List distributed apps.

GET

List distributed apps, including distributed state information.

Request parameters

Name	Type	Default	Description
clientId	String		Select apps that match *clientId.*
hasDeploymentError	Boolean		Select apps according to deployment fault status: `0` = Do not include apps with a deployment fault indication. `1` = Include apps with a deployment fault indication.

Pagination and filtering parameters can be used with this method.

Returned values

The response includes these values for each app listed.

Name	Description
archive	Disk location of the archived version of the app.
clientId	Deployment client ID associated with the app, an MD5 hash value of serialized (catenated) client attributes.

Name	Description
hasDeploymentError	Indicates deployment fault status on at least one deployment client: `0` = Do not include apps with a deployment fault indication. `1` = Include apps with a deployment fault indication.
loadtime	Last deployment server app loaded or reloaded date and time. An application not mapped to *serverclasses* is not loaded so *loadtime* is `0`.
restartSplunkWeb	Restart Splunk Web indication: `0` = Do not restart Splunk Web. `1` = Restart Splunk Web.
restartSplunkd	Restart splunkd indication: `0` = Do not restart splunkd. `1` = Restart splunkd.
serverclasses	List of server classes associated with the application.
size	Size on disk of the compressed app (bundle), in bytes.
stateOnClient	App enablement status: `0` = Not enabled. `1` = Enabled.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/applications
```

XML Response

```
...
 <title>applications</title>
 <id>https://localhost:8089/services/deployment/server/applications</id>
 <updated>2013-08-01T09:35:22-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/applications/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>wma-app-test2</title>
   <id>https://localhost:8089/services/deployment/server/applications/wma-app2</id>
   <updated>2013-08-01T09:35:22-07:00</updated>
   <link href="/services/deployment/server/applications/wma-app2" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <content type="text/xml">
     <s:dict>
       <s:key name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app2-1375305443.bundle</s:key>
       ... eai:acl node elided ...
       <s:key name="loadtime">Wed Jul 31 14:17:23 2013</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
```

```
        <s:key name="restartSplunkd">0</s:key>
        <s:key name="serverclasses">
          <s:list>
            <s:item>sc_mach_type</s:item>
            <s:item>sc_new</s:item>
            <s:item>sc_apps_wma</s:item>
          </s:list>
        </s:key>
        <s:key name="size">112640</s:key>
        <s:key name="stateOnClient">enabled</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>wma-app1</title>
    <id>https://localhost:8089/services/deployment/server/applications/wma-app1</id>
    <updated>2013-08-01T09:35:22-07:00</updated>
    <link href="/services/deployment/server/applications/wma-app_test1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <content type="text/xml">
      <s:dict>
        <s:key name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app1-1375305443.bundle</s:key>
        ... eai:acl node elided ...
        <s:key name="loadtime">Wed Jul 31 14:17:23 2013</s:key>
        <s:key name="restartSplunkWeb">0</s:key>
        <s:key name="restartSplunkd">0</s:key>
        <s:key name="serverclasses">
          <s:list>
            <s:item>sc_new</s:item>
            <s:item>sc_apps_wma</s:item>
          </s:list>
        </s:key>
        <s:key name="size">112640</s:key>
        <s:key name="stateOnClient">enabled</s:key>
      </s:dict>
    </content>
  </entry>
```

deployment/server/applications/{name}

`https://<host>:<mPort>/services/deployment/server/applications/{name}`

Get or update distribution information for `{name}` app.

GET

Get `{name}` app distribution information.

Request parameters

None

Returned values

Name	Description
archive	Disk location of archived version of the app.
clientId	Deployment client ID associated with the app, an MD5 hash value of serialized (catenated) client attributes.
hasDeploymentError	Indicates deployment fault status on at least one deployment client: `0` = Do not include apps with a deployment fault indication. `1` = Include apps with a deployment fault indication.
loadtime	Last deployment server app loaded or reloaded date and time. An application not mapped to *serverclasses* is not loaded so *loadtime* is `0`.
restartSplunkWeb	Restart Splunk Web indication: `0` = Do not restart Splunk Web. `1` = Restart Splunk Web.
restartSplunkd	Restart splunkd indication: `0` = Do not restart splunkd. `1` = Restart splunkd.
serverclasses	List of server classes associated with the application.
size	Size on disk of the compressed app (bundle), in bytes.
stateOnClient	App enablement status: `0` = Not enabled. `1` = Enabled.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/applications/wma-app1
```

XML Response

```
...
 <title>applications</title>
 <id>https://localhost:8089/services/deployment/server/applications</id>
 <updated>2013-08-04T18:53:50-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/applications/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>wma-app1</title>
   <id>https://localhost:8089/services/deployment/server/applications/wma-app1</id>
   <updated>2013-08-04T18:53:50-07:00</updated>
   <link href="/services/deployment/server/applications/wma-app1" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <content type="text/xml">
     <s:dict>
       <s:key name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app1-1375467593.bundle</s:key>
```

```
      ... eai:acl node elided ...
      <s:key name="eai:attributes">... elided ...</s:key>
      <s:key name="loadtime">Fri Aug  2 11:19:53 2013</s:key>
      <s:key name="restartSplunkWeb">0</s:key>
      <s:key name="restartSplunkd">0</s:key>
      <s:key name="serverclasses">
        <s:list>
          <s:item>sc_new</s:item>
          <s:item>sc_apps_wma</s:item>
        </s:list>
      </s:key>
      <s:key name="size">112640</s:key>
      <s:key name="stateOnClient">enabled</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update `{name}` app distribution information.

Usage details
When *continueMatching* is `true`, matching is in the order in which server classes are defined.

The *whitelist* setting indicates a filtering strategy that includes a subset.

- Items are not considered to match the server class by default.
- Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class.
- Items that match any blacklist entry are not considered to match the server class, regardless of whitelist.

The *blacklist* setting indicates a filtering strategy that excludes a subset.

- Items are considered to match the server class by default.
- Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class.
- Items that match any whitelist entry are considered to match the server class.

That is,

whitelist: default no-match -> whitelists enable -> blacklists disable
blacklist: default match -> blacklists disable-> whitelists enable

If you specify whitelist at the global level, and then specify blacklist for an individual server class, the setting becomes blacklist for that server class, and you have to provide another filter in that server class definition to replace the one you overrode.

Request parameters

Name	Type	Default	Description

*blacklist.**	String		List of hosts to exclude when mapping application to a server class. For each *blacklist*, replace the wildcard (*) with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.
continueMatching	Boolean		Configuration layering indication, across classes and server-specific settings: `true` = [Default] Configuration lookups continue matching server classes after the first match. `false` = Use the first match, only.
deinstall	Boolean		Remove mapping indication: `true` = Remove mapping of {name} from all server classes and delete it from client target repositories. `false` = Do not remove mapping of {name}.
filterType	Enum		Filter execution order: `whitelist` = Whitelist filters are applied before blacklist filters. `blacklist` = Blacklist filters are applied before whitelist filters.
machineTypesFilter	String		Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters. Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included. Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter. The patterns are PCRE regular expressions, with the following aids for easier entry: • You can specify '.' to mean '\\.' • You can specify '*' to mean '.*' • Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.
repositoryLocation	String		The location on the deployment server to store the content that is to be deployed for this server class. For example: $SPLUNK_HOME/etc/deployment-apps
restartSplunkWeb	Boolean		Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated. Defaults to false
restartSplunkd	Boolean		Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated. Defaults to false
serverclass	String		The name of the server class to which the application is mapped. Do not specify this parameter if `deinstall` is true.
stateOnClient	Enum		Valid values are (enabled | disabled | noop). • *enabled*: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server. • *disabled*: Sets the application state to disabled on the client, regardless of state on the deployment server. • *noop*: The state on the client is the same as on the deployment server.

Name	Type	Default	Description
targetRepositoryLocation	String		The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used. That is, defaults to: $SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk deployment) Useful only with complex (for example, tiered) deployment strategies.
tmpFolder	String		Working folder used by deployment server. Defaults to $SPLUNK_HOME/var/run/tmp
unmap	Boolean		Indicates whether to remove the mapping of the application to the specified server class.
*whitelist.**	String		List of hosts to accept for this server class. For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.

Returned values

Name	Description
archive	Specifies the location of the compressed version (*bundle*) of the app.
*blacklist.**	Regular expressions used to exclude, when mapping this application to a client. If a client matches any of the blacklist regular expressions, it does not receive the application. The * is replaced by an integral ordinal number.
continueMatching	If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used.
filterType	blacklist) Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters. See description for the filterType POST parameter for more information.
loadtime	Specifies the date and time the application was last loaded (or reloaded) by the deployment server. An application not mapped to any serverclasses does not get loaded, thus its loadtime attribute is 0; in epoch terms, which is 01 Jan 1970 at midnight GMT.
machineTypesFilter	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
repositoryLocation	The location on the deployment server to store the content that is to be deployed for this server class.
restartSplunkWeb	Indicates whether to restart Splunk Web.
restartSplunkd	Indicates whether to restart splunkd.

Name	Description
serverclass	The name of the server class to which the application is mapped.
serverclasses	List of server classes associated with the application.
size	Indicates in bytes the size on disk of the compressed version (*bundle*) of the application.
stateOnClient	Specifies whether the deployment client is enabled or disabled.
targetRepositoryLocation	The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used.
tmpFolder	Working folder used by deployment server.
*whitelist.**	Regular expressions used to accept, when mapping this application to a client. If a client matches any of the whitelist regular expressions, it accepts the application. The * is replaced by an integral ordinal number.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/applications/wma-app3 -d
serverclass=sc_apps_wma
```

XML Response

```
...
 <title>applications</title>
 <id>https://localhost:8089/services/deployment/server/applications</id>
 <updated>2013-08-10T12:50:59-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/applications/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>wma-app3</title>
   <id>https://localhost:8089/services/deployment/server/applications/wma-app3</id>
   <updated>2013-08-10T12:50:59-07:00</updated>
   <link href="/services/deployment/server/applications/wma-app3" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <content type="text/xml">
     <s:dict>
       <s:key
name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_mach_type/wma-app3-1376164259.bundle</s:key>
       ... eai:acl node elided ...
       <s:key name="loadtime">Sat Aug 10 12:50:59 2013</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
```

```
      <s:key name="restartSplunkd">0</s:key>
      <s:key name="serverclasses">
        <s:list>
          <s:item>sc_mach_type</s:item>
          <s:item>sc_apps_wma</s:item>
        </s:list>
      </s:key>
      <s:key name="size">112640</s:key>
      <s:key name="stateOnClient">enabled</s:key>
    </s:dict>
  </content>
</entry>
```

deployment/server/clients

`https://<host>:<mPort>/services/deployment/server/clients`
Provides access to information about clients to a deployment server.

GET

Access information about clients to a deployment server.

Request parameters

Name	Type	Default	Description
action	String		Use one of the following values: • `phonehome`: deployment client is verifying app status (typical state) • `unknown`: app state on deployment client restart • `download`: deployment client is downloading the app or app update • `install`: deployment client is installing or updating the app • `uninstall` app removed from deployment server, marked for uninstall on the deployment client The GET response includes all clients with an app that has the specified action.
application	String		Lists clients to the deployment server that have attempted to download the named application.
hasDeploymentError	Boolean	False	Indicates whether to list only clients that have a deployment error.
maxPhonehome_latency_to_avgInterval_ratio	Number		List clients to the deployment server when the ratio of the phone home latency to the average phone home interval is less than the value supplied to this parameter.
minLatestPhonehomeTime	Number		Lists clients for which there is a phone home message at the specified time or later, in epoch seconds. That is, list the client for the following condition:

Name	Type	Default	Description
			client latency ? (now?minLatestPhonehomeTime)
minPhonehome_latency_to_avgInterval_ratio	Number		List clients to the deployment server when the ratio of the phone home latency to the average phone home interval is greater than the value supplied with this parameter.
serverclasses	String		Comma-separated list of serverclasses. List clients that are configured to receive an application to a listed serverclass. The match is a logical OR of, for each Si, include C if C is sent an app A that maps to Si in serverclass.conf, if such an app existed. The "would have" is per blacklist.n or whitelist.n/machineTypesFilter in serverclass.conf

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
applications	List of applications deployed to the deployment client.
averagePhoneHomeInterval	The average phone home interval, in seconds.
build	The build number for the Splunk instance on the deployment client.
dns	The DNS lookup name of the deployment client server.
guid	Identifier for the deployment server client.
hasDeploymentError	Specifies whether to check for clients with a deployment error.
hostname	The host name of the deployment client server.
id	ID for the client based on client name and IP address.
ip	The IP address of the client to the deployment server.
lastPhoneHomeTime	The last time the deployment client phones home to the deployment server, in epoch time.
mgmt	The managment port for the deployment client.
minLatestPhonehomeTime	Specifies in epoch seconds the minimum latency for a client to contact the deployment server.
minPhonehome_latency_to_avgInterval_ratio	The minimum value specified for the ratio of the phone home latency to the average phone home interval.
name	The name of the deployment client server.
serverclasses	List of server classes for the deployment client.
utsname	Machine type for the deployment server client.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/clients
```

XML Response

```
<title>serverclients</title>
 <id>https://localhost:8089/services/deployment/server/clients</id>
 <updated>2013-08-01T09:41:42-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/clients/countClients_by_machineType"
rel="countClients_by_machineType"/>
 <link href="/services/deployment/server/clients/countRecentDownloads" rel="countRecentDownloads"/>
 <link href="/services/deployment/server/clients/getMatchingAppsForClient_dryRun"
rel="getMatchingAppsForClient_dryRun"/>
 <link href="/services/deployment/server/clients/preview" rel="preview"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>dc95537d0e8fdadc44d00c50fc431e25</title>
   <id>https://localhost:8089/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25</id>
   <updated>2013-08-01T09:41:42-07:00</updated>
   <link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="list"/>
   <link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="applications">
         <s:dict>
           <s:key name="wma-app-test2">
             <s:dict>
               <s:key name="action">Install</s:key>
               <s:key
name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app2-1375305443.bundle</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="result">Ok</s:key>
               <s:key name="serverclasses">
                 <s:list>
                   <s:item>sc_mach_type</s:item>
                   <s:item>sc_new</s:item>
                   <s:item>sc_apps_wma</s:item>
                 </s:list>
               </s:key>
               <s:key name="size">112640</s:key>
               <s:key name="stateOnClient">enabled</s:key>
               <s:key name="timestamp">Wed Jul 31 14:11:23 2013</s:key>
             </s:dict>
           </s:key>
           <s:key name="wma-app_test1">
             <s:dict>
               <s:key name="action">Install</s:key>
               <s:key
name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app1-1375305443.bundle</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="result">Ok</s:key>
               <s:key name="serverclasses">
                 <s:list>
                   <s:item>sc_new</s:item>
                   <s:item>sc_apps_wma</s:item>
                 </s:list>
               </s:key>
               <s:key name="size">112640</s:key>
               <s:key name="stateOnClient">enabled</s:key>
               <s:key name="timestamp">Wed Jul 31 14:17:23 2013</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="averagePhoneHomeInterval">60</s:key>
       <s:key name="build">172889</s:key>
       <s:key name="dns">localhost.sv.splunk.com</s:key>
       ... eai:acl node elided ...
       <s:key name="guid">dc95537d0e8fdadc44d00c50fc431e25</s:key>
       <s:key name="hostname">localhost.sv.splunk.com</s:key>
       <s:key
name="id">connection_10.160.24.187_8089_localhost.sv.splunk.com_localhost.sv.splunk.com_Ombra</s:key>
       <s:key name="ip">10.160.24.187</s:key>
       <s:key name="lastPhoneHomeTime">1375375291</s:key>
       <s:key name="mgmt">8089</s:key>
       <s:key name="name">Ombra</s:key>
       <s:key name="serverClasses">
         <s:dict>
           <s:key name="sc_apps_wma">
             <s:dict>
               <s:key name="loadTime">1375305443</s:key>
               <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
           <s:key name="sc_mach_type">
             <s:dict>
               <s:key name="loadTime">1375305443</s:key>
               <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
           <s:key name="sc_new">
             <s:dict>
               <s:key name="loadTime">1375305443</s:key>
               <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="utsname">linux-x86_64</s:key>
     </s:dict>
   </content>
 </entry>
```

deployment/server/clients/countClients_by_machineType

`https://<host>:<mPort>/services/deployment/server/clients/countClients_by_machineType`
Access information about deployment clients to this server according to the machine type of the client.

GET

List the count of deployment clients for this server by machine type.

Request parameters

None

Returned values

Name	Description
counts	The list of machine types for this deployment client, showing the count of each machine type.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/clients/countClients_by_machineType
```

XML Response

```
 <title>serverclients</title>
 <id>https://localhost:8089/services/deployment/server/clients</id>
 <updated>2013-07-30T15:07:38-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/clients/countClients_by_machineType"
rel="countClients_by_machineType"/>
 <link href="/services/deployment/server/clients/countRecentDownloads" rel="countRecentDownloads"/>
 <link href="/services/deployment/server/clients/getMatchingAppsForClient_dryRun"
rel="getMatchingAppsForClient_dryRun"/>
 <link href="/services/deployment/server/clients/preview" rel="preview"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>default</title>
   <id>https://localhost:8089/services/deployment/server/clients/default</id>
   <updated>2013-07-30T15:07:38-07:00</updated>
   <link href="/services/deployment/server/clients/default" rel="alternate"/>
   <author>
```

```
    <name>system</name>
  </author>
  <link href="/services/deployment/server/clients/default" rel="list"/>
  <link href="/services/deployment/server/clients/default" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="counts">
        <s:dict>
          <s:key name="linux-x86_64">3</s:key>
        </s:dict>
      </s:key>
      ... eai:acl node elided ...
    </s:dict>
  </content>
</entry>
```

deployment/server/clients/countRecentDownloads

`https://<host>:<mPort>/services/deployment/server/clients/countRecentDownloads`

Access the count of the number of downloads from this client to the deployment server during the last specified time period.

GET

Return the count of the number of downloads from this client to the deployment server during the last specified time period.

Request parameters

Name	Type	Default	Description
maxAgeSecs required	Number		Age of the downloads to count, in seconds.

Returned values

Name	Description
count	The number of recent downloads.

Example request and response

XML Request

```
curl -k -u admin:pass -d maxAgeSecs=1 -G
https://localhost:8089/services/deployment/server/clients/countRecentDownloads
```

XML Response

```
...
 <title>serverclients</title>
 <id>https://localhost:8089/services/deployment/server/clients</id>
 <updated>2013-07-30T20:00:43-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/clients/countClients_by_machineType"
rel="countClients_by_machineType"/>
 <link href="/services/deployment/server/clients/countRecentDownloads" rel="countRecentDownloads"/>
 <link href="/services/deployment/server/clients/getMatchingAppsForClient_dryRun"
rel="getMatchingAppsForClient_dryRun"/>
 <link href="/services/deployment/server/clients/preview" rel="preview"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>default</title>
   <id>https://localhost:8089/services/deployment/server/clients/default</id>
   <updated>2013-07-30T20:00:43-07:00</updated>
   <link href="/services/deployment/server/clients/default" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/server/clients/default" rel="list"/>
   <link href="/services/deployment/server/clients/default" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="count">6</s:key>
       ... eai:acl node elided ...
     </s:dict>
   </content>
 </entry>
```

deployment/server/clients/{name}

`https://<host>:<mPort>/services/deployment/server/clients/{name}`

Get client information or remove a client.

DELETE

Remove the specified client from the deployment server registry. The next time the client "phones home" the record is re-created.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/deployment/server/clients/1d3de43af2aae61139c367044127f44a
```

XML Response

```
...
 <title>serverclients</title>
 <id>https://qa-sv-rh61x64-7:8103/services/deployment/server/clients</id>
 <updated>2013-10-21T16:03:49-07:00</updated>
 <generator build="182785" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/clients/countClients_by_machineType"
rel="countClients_by_machineType"/>
 <link href="/services/deployment/server/clients/countRecentDownloads" rel="countRecentDownloads"/>
 <link href="/services/deployment/server/clients/getMatchingAppsForClient_dryRun"
rel="getMatchingAppsForClient_dryRun"/>
 <link href="/services/deployment/server/clients/preview" rel="preview"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>149685cb3e39898fbd15be6604672a31</title>
   <id>https://qa-sv-rh61x64-7:8103/services/deployment/server/clients/149685cb3e39898fbd15be6604672a31</id>
   <updated>2013-10-21T16:03:49-07:00</updated>
   <link href="/services/deployment/server/clients/149685cb3e39898fbd15be6604672a31" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/server/clients/149685cb3e39898fbd15be6604672a31" rel="list"/>
   <link href="/services/deployment/server/clients/149685cb3e39898fbd15be6604672a31" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="averagePhoneHomeInterval">60</s:key>
       <s:key name="build">177748</s:key>
       <s:key name="clientName">4D4EA12E-FDBA-41D3-99CD-2A61CC1DAB29</s:key>
       <s:key name="dns">qa-sv-rh61x64-10.sv.splunk.com</s:key>
       ... eai:acl node elided ...
       <s:key name="guid">149685cb3e39898fbd15be6604672a31</s:key>
       <s:key name="hostname">qa-sv-rh61x64-10</s:key>
       <s:key
name="id">connection_10.160.24.224_8097_qa-sv-rh61x64-10.sv.splunk.com_qa-sv-rh61x64-10_4D4EA12E-FDBA-41D3-99CD
-2A61CC1DAB29</s:key>
       <s:key name="ip">10.160.24.224</s:key>
       <s:key name="lastPhoneHomeTime">1382396628</s:key>
       <s:key name="mgmt">8097</s:key>
       <s:key name="name">4D4EA12E-FDBA-41D3-99CD-2A61CC1DAB29</s:key>
       <s:key name="serverClasses"/>
       <s:key name="utsname">linux-x86_64</s:key>
     </s:dict>
   </content>
 </entry>
 . . . elided ...
```

GET

Lists information about the named client to the deployment server.

Request parameters

Name	Type	Default	Description
application	String		Lists information about this client with respect to the named application.
hasDeploymentError	Boolean		Indicates whether to list this client if has a deployment error.
maxPhonehome_latency_to_avgInterval_ratio	Number		List clients to the deployment server when the ratio of the phone home latency to the average phone home interval is less than the value supplied to this parameter.
minLatestPhonehomeTime	Number		Specifies in epoch seconds the minimum latency for a client to contact the deployment server. This endpoint lists information about the named client if it has a latency equal to or greater than specified by this parameter.
minPhonehome_latency_to_avgInterval_ratio	Number		List information about the named client to the deployment server when the ratio of the phone home latency to the average phone home interval is greater than the value supplied with this parameter.
serverclasses	String		Comma-separated list of serverclasses. Lists information about this client if it is configured to send an application to a listed serverclass.

Returned values

Name	Description
application	The name of the application specified to filter the results of this call.
applications	List of applications deployed to the deployment client.
averagePhoneHomeInterval	The average phone home interval, in seconds.
build	The build number for the Splunk instance on the deployment client.
dns	The DNS lookup name of the deployment client server.
guid	Identifier for the deployment server client.
hasDeploymentError	Specifies whether to check for clients with a deployment error.
hostname	The host name of the deployment client server.
id	ID for the client based on client name and IP address.
ip	The IP address of the client to the deployment server.
lastPhoneHomeTime	The last time the deployment client phones home to the deployment server, in epoch time.
maxPhonehome_latency_to_avgInterval_ratio	The maximum value specified for the ratio of the phone home latency to the average phone home interval.
mgmt	The managment port for the deployment client.

Name	Description
minLatestPhonehomeTime	Specifies in epoch seconds the minimum latency for a client to contact the deployment server.
minPhonehome_latency_to_avgInterval_ratio	The minimum value specified for the ratio of the phone home latency to the average phone home interval.
name	The name of the deployment client server.
serverClasses	The list of server classes to which the client belongs.
serverclasses	List of server classes for the deployment client.
utsname	Machine type for the deployment server client.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25
```

XML Response

```
...
 <title>serverclients</title>
 <id>https://localhost:8089/services/deployment/server/clients</id>
 <updated>2013-08-04T18:59:31-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/clients/countClients_by_machineType"
rel="countClients_by_machineType"/>
 <link href="/services/deployment/server/clients/countRecentDownloads" rel="countRecentDownloads"/>
 <link href="/services/deployment/server/clients/getMatchingAppsForClient_dryRun"
rel="getMatchingAppsForClient_dryRun"/>
 <link href="/services/deployment/server/clients/preview" rel="preview"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>dc95537d0e8fdadc44d00c50fc431e25</title>
   <id>https://localhost:8089/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25</id>
   <updated>2013-08-04T18:59:31-07:00</updated>
   <link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="list"/>
   <link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="applications">
         <s:dict>
           <s:key name="wma-app2">
             <s:dict>
               <s:key name="action">Unknown</s:key>
               <s:key
```

```
name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app2-1375467593.bundle</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="result">Ok</s:key>
               <s:key name="serverclasses">
                 <s:list>
                   <s:item>sc_mach_type</s:item>
                   <s:item>sc_new</s:item>
                   <s:item>sc_apps_wma</s:item>
                 </s:list>
               </s:key>
               <s:key name="size">112640</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
           <s:key name="wma-app1">
             <s:dict>
               <s:key name="action">Unknown</s:key>
               <s:key
name="archive">/opt/cluster/peer1/splunk/var/run/tmp/sc_new/wma-app1-1375467593.bundle</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="result">Ok</s:key>
               <s:key name="serverclasses">
                 <s:list>
                   <s:item>sc_new</s:item>
                   <s:item>sc_apps_wma</s:item>
                 </s:list>
               </s:key>
               <s:key name="size">112640</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="averagePhoneHomeInterval">60</s:key>
       <s:key name="build">172889</s:key>
       <s:key name="dns">localhost.sv.splunk.com</s:key>
       ... eai:acl node elided ...
       ... eai:attribute node elided ...
       <s:key name="guid">dc95537d0e8fdadc44d00c50fc431e25</s:key>
       <s:key name="hostname">localhost.sv.splunk.com</s:key>
       <s:key
name="id">connection_10.160.24.187_8089_localhost.sv.splunk.com_localhost.sv.splunk.com_Ombra</s:key>
       <s:key name="ip">10.160.24.187</s:key>
       <s:key name="lastPhoneHomeTime">1375667964</s:key>
       <s:key name="mgmt">8089</s:key>
       <s:key name="name">Ombra</s:key>
       <s:key name="serverClasses">
         <s:dict>
           <s:key name="sc_apps_wma">
             <s:dict>
               <s:key name="loadTime">1375467593</s:key>
               <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
           <s:key name="sc_mach_type">
             <s:dict>
               <s:key name="loadTime">1375467593</s:key>
               <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
           <s:key name="sc_new">
             <s:dict>
               <s:key name="loadTime">1375467593</s:key>
               <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
               <s:key name="restartSplunkWeb">0</s:key>
               <s:key name="restartSplunkd">0</s:key>
               <s:key name="stateOnClient">enabled</s:key>
             </s:dict>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="utsname">linux-x86_64</s:key>
     </s:dict>
   </content>
 </entry>
```

deployment/server/config

`https://<host>:<mPort>/services/deployment/server/config`

Access server configuration information for deployment servers.

POST

List configuration information for all deployment servers.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
currentDownloads	The number of current downloads for this deployment server.
disabled	Indicates whether the deployment server is disabled.
loadTime	The time, in epoch seconds, the serverclass for this server was loaded.
repositoryLocation	The location on the deployment server to store the content that is to be deployed.
whitelist.0	Lists the contents of whitelist.0.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/config
```

XML Response

```
...
 <title>deploymentserver</title>
 <id>https://localhost:8089/services/deployment/server/config</id>
 <updated>2013-08-01T08:17:38-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/config/_reload" rel="_reload"/>
 <link href="/services/deployment/server/config/attributesUnsupportedInUI" rel="attributesUnsupportedInUI"/>
 <link href="/services/deployment/server/config/listIsDisabled" rel="listIsDisabled"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>config</title>
   <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/config/config</id>
   <updated>2013-08-01T08:17:38-07:00</updated>
   <link href="/servicesNS/nobody/system/deployment/server/config/config" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/deployment/server/config/config" rel="list"/>
   <link href="/servicesNS/nobody/system/deployment/server/config/config/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/deployment/server/config/config" rel="edit"/>
   <link href="/servicesNS/nobody/system/deployment/server/config/config/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="currentDownloads">0</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl node elided ...
       <s:key name="loadTime">1375305443</s:key>
       <s:key name="repositoryLocation">$SPLUNK_HOME/etc/deployment-apps</s:key>
       <s:key name="whitelist.0">*</s:key>
     </s:dict>
   </content>
 </entry>
```

deployment/server/config/attributesUnsupportedInUI

```
https://<host>:<mPort>/services/deployment/server/config/attributesUnsupportedInUI
```

Access deployment server attributes that cannot be configured from Splunk Web.

GET

Lists deployment server attributes that cannot be configured from Splunk Web.

Request parameters
None

Returned values

Name	Description
property	The attribute that cannot be configured from Splunk Web.
reason	The reason an attribute cannot be configured from Splunk Web.
stanza	In Splunk Enterprise, the stanza in `serverclass.conf` that lists deployment server attributes that cannot be configured from Splunk Web.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/config/attributesUnsupportedInUI
```

XML Response

```
...
 <title>deploymentserver</title>
 <id>https://localhost:8089/services/deployment/server/config</id>
 <updated>2013-08-04T19:14:20-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/config/_reload" rel="_reload"/>
 <link href="/services/deployment/server/config/attributesUnsupportedInUI" rel="attributesUnsupportedInUI"/>
 <link href="/services/deployment/server/config/listIsDisabled" rel="listIsDisabled"/>
 ... eai:acl node elided ...
 <s:messages/>
 <entry>
   <title>item_0</title>
   <id>https://localhost:8089/services/deployment/server/config/item_0</id>
   <updated>2013-08-04T19:14:20-07:00</updated>
   <link href="/services/deployment/server/config/item_0" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/server/config/item_0" rel="list"/>
   <link href="/services/deployment/server/config/item_0/_reload" rel="_reload"/>
   <link href="/services/deployment/server/config/item_0" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       ... opensearch nodes elided ...
       <s:key name="property">whitelist.0</s:key>
       <s:key name="reason">unsupported at this level</s:key>
```

```
      <s:key name="stanza">global</s:key>
    </s:dict>
  </content>
</entry>
```

deployment/server/config/listIsDisabled

`https://<host>:<mPort>/services/deployment/server/config/listIsDisabled`

Access deployment server enablement status.

GET

Access deployment server enablement status.

Request parameters

None

Request parameters

Name	Description
disabled	Indicates if the deployment server is disabled.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/config/listIsDisabled
```

XML Response

```
...
 <title>deploymentserver</title>
 <id>https://localhost:8089/services/deployment/server/config</id>
 <updated>2013-08-10T14:08:11-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/config/_reload" rel="_reload"/>
 <link href="/services/deployment/server/config/attributesUnsupportedInUI" rel="attributesUnsupportedInUI"/>
 <link href="/services/deployment/server/config/listIsDisabled" rel="listIsDisabled"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>default</title>
   <id>https://localhost:8089/services/deployment/server/config/default</id>
   <updated>2013-08-10T14:08:11-07:00</updated>
```

```
    <link href="/services/deployment/server/config/default" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/deployment/server/config/default" rel="list"/>
    <link href="/services/deployment/server/config/default/_reload" rel="_reload"/>
    <link href="/services/deployment/server/config/default" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
```

deployment/server/serverclasses

`https://<host>:<mPort>/services/deployment/server/serverclasses`

Access information about server classes.

GET

List server classes for this deployment server.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
blacklist-size	The number of entires in the blacklist for this serverclass.
clientId	ID of deployment client for this server class.
currentDownloads	Number of applications currently downloaded.
hasDeploymentError	Indicates whether the serverclass has at least one deployment error.
loadTime	The time, in epoch seconds, this serverclass was loaded.
machineTypesFilter	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
repositoryList	List of applications stored at the location specified by repositoryLocation.
repositoryLocation	The location on the deployment server to store the content that is to be deployed for this server class.
restartSplunkWeb	Indicates whether to restart Splunk Web.
restartSplunkd	Indicates whether to restart splunkd.
stateOnClient	Indicates whether this server class is enabled or disabled.
whitelist-size	Specifies the number of entries in the whitelist for this server class.

Name	Description
whitelist.0	List of servers for whitelist.0 for this server class.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses
```

XML Response

```
...
 <title>serverclasses</title>
 <id>https://localhost:8089/services/deployment/server/serverclasses</id>
 <updated>2013-08-01T09:50:16-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/serverclasses/_new" rel="create"/>
 <link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>sc_apps_wma</title>
   <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma</id>
   <updated>2013-08-01T09:50:16-07:00</updated>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="list"/>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="edit"/>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="remove"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_apps_wma/applications"
rel="applications"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_apps_wma/clients" rel="clients"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_apps_wma/reload" rel="reload"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="blacklist-size">0</s:key>
       <s:key name="currentDownloads">0</s:key>
       ... eai:acl node elided ...
       <s:key name="loadTime">1375305443</s:key>
       <s:key name="machineTypesFilter"></s:key>
       <s:key name="repositoryList">
         <s:dict>
           <s:key name="wma-app2"/>
           <s:key name="wma-app1"/>
         </s:dict>
       </s:key>
       <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
       <s:key name="restartSplunkd">0</s:key>
       <s:key name="stateOnClient">enabled</s:key>
       <s:key name="whitelist-size">1</s:key>
```

```
        <s:key name="whitelist.0">Ombra*</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>sc_mach_type</title>
    <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type</id>
    <updated>2013-08-01T09:50:16-07:00</updated>
    <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="list"/>
    <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="edit"/>
    <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="remove"/>
    <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_mach_type/applications"
rel="applications"/>
    <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_mach_type/clients" rel="clients"/>
    <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_mach_type/reload" rel="reload"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="blacklist-size">0</s:key>
        <s:key name="currentDownloads">0</s:key>
        ... eai:acl node elided ...
        <s:key name="loadTime">1375305443</s:key>
        <s:key name="machineTypesFilter">linux-x86_64,</s:key>
        <s:key name="repositoryList">
          <s:dict>
            <s:key name="wma-app-test2"/>
            <s:key name="wma-app_test1"/>
          </s:dict>
        </s:key>
        <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
        <s:key name="restartSplunkWeb">0</s:key>
        <s:key name="restartSplunkd">0</s:key>
        <s:key name="stateOnClient">enabled</s:key>
        <s:key name="whitelist-size">1</s:key>
        <s:key name="whitelist.0">Ombra*</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create a server class.

Request parameters

Name	Type	Default	Description
name required	String		The name of the server class.
*blacklist.**	String		List of hosts to exclude for this server class.

Name	Type	Default	Description
			For each blacklist, replace * with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.
continueMatching	Boolen		Controls how configuration is layered across classes and server-specific settings. If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used. Matching is done in the order that server classes are defined. Defaults to true. A serverClass can override this property and stop the matching.
filterType	Enum		Valid values: (whitelist | blacklist) Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters. The whitelist setting indicates a filtering strategy that pulls in a subset: • Items are not considered to match the server class by default. • Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class. • Items that match any blacklist entry are not considered to match the server class, regardless of whitelist. The blacklist setting indicates a filtering strategy that rules out a subset: • Items are considered to match the server class by default. • Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class. • Items that match any whitelist entry are considered to match the server class. More briefly: whitelist: default no-match -> whitelists enable -> blacklists disable blacklist: default match -> blacklists disable-> whitelists enable If you specify whitelist at the global level, and then specify blacklist for an individual server class, the setting becomes blacklist for that server class, and you have to provide another filter in that server class definition to replace the one you overrode.
machineTypesFilter	String		Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters. Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included. Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter. The patterns are PCRE regular expressions, with the following aids for easier entry:

Name	Type	Default	Description
			• You can specify '.' to mean '\\.' • You can specify '*' to mean '.*' • Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.
repositoryLocation	String		The location on the deployment server to store the content that is to be deployed for this server class. For example: $SPLUNK_HOME/etc/deployment-apps
restartSplunkWeb	Boolean		Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated. Defaults to false
restartSplunkd	Boolean		Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated. Defaults to false
stateOnClient	Enum		Valid values are (enabled | disabled | noop). • *enabled*: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server. • *disabled*: Sets the application state to disabled on the client, regardless of state on the deployment server. • *noop*: The state on the client is the same as on the deployment server.
targetRepositoryLocation	String		The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used. That is, defaults to: $SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk instance Useful only with complex (for example, tiered) deployment strategies.
tmpFolder	String		Working folder used by deployment server. Defaults to $SPLUNK_HOME/var/run/tmp
*whitelist.**	String		List of hosts to accept for this server class. For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.

Returned values

Name	Description
blacklist-size	The number of entries in the blacklist for this serverclass.
*blacklist.**	Regular expressions used to exclude for this server class.

Name	Description
	If a client matches any of the blacklist regular expressions, it is not included in the server class. The * is replaced by an integral ordinal number.
continueMatching	If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used.
currentDownloads	Number of applications currently downloaded.
filterType	blacklist) Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters. See description for the filterType POST parameter for more information.
loadTime	The time, in epoch seconds, this serverclass was loaded.
machineTypesFilter	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
repositoryList	List of applications stored at the location specified by repositoryLocation.
repositoryLocation	The location on the deployment server to store the content that is to be deployed for this server class.
restartSplunkWeb	Indicates whether to restart Splunk Web.
restartSplunkd	Indicates whether to restart splunkd.
stateOnClient	Specifies whether the deployment client is enabled or disabled.
targetRepositoryLocation	The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used. That is, defaults to: $SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk deployment. Useful only with complex (for example, tiered) deployment strategies.
tmpFolder	Working folder used by deployment server. Defaults to $SPLUNK_HOME/var/run/tmp
whitelist-size	Specifies the number of entries in the whitelist for this server class.
*whitelist.**	Regular expressions used to accept for this server class. If a client matches any of the whitelist regular expressions, it is included in the server class. The * is replaced by an integral ordinal number.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses -d name=sc_apps_ombra
```

XML Response

```
...
 <title>serverclasses</title>
 <id>https://localhost:8089/services/deployment/server/serverclasses</id>
 <updated>2013-08-10T13:18:28-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/serverclasses/_new" rel="create"/>
 <link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>sc_apps_ombra</title>
   <id>https://localhost:8089/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra</id>
   <updated>2013-08-10T13:18:28-07:00</updated>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra" rel="list"/>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra" rel="edit"/>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra" rel="remove"/>
   <link href="/servicesNS/nobody/search/deployment/serverclasses/sc_apps_ombra/applications"
rel="applications"/>
   <link href="/servicesNS/nobody/search/deployment/serverclasses/sc_apps_ombra/clients" rel="clients"/>
   <link href="/servicesNS/nobody/search/deployment/serverclasses/sc_apps_ombra/reload" rel="reload"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="blacklist-size">0</s:key>
       <s:key name="currentDownloads">0</s:key>
       ... opensearch nodes elided ...
       <s:key name="loadTime">1376165908</s:key>
       <s:key name="machineTypesFilter"></s:key>
       <s:key name="repositoryList">
         <s:dict>
           <s:key name="wma-app-test2"/>
           <s:key name="wma-app3"/>
           <s:key name="wma-app_test1"/>
         </s:dict>
       </s:key>
       <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
       <s:key name="restartSplunkd">0</s:key>
       <s:key name="stateOnClient">enabled</s:key>
       <s:key name="whitelist-size">0</s:key>
     </s:dict>
   </content>
 </entry>
```

deployment/server/serverclasses/rename

`https://<host>:<mPort>/services/deployment/server/serverclasses/rename`
Rename a server class.

POST

Specify a new name for a server class.

Request parameters

Name	Type	Default	Description
newName required	String		The new name of the server class.
oldName required	String		The current name of the server class.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses/rename -d
oldName=sc_apps_ombra -d newName=sc_apps_shadow
```

XML Response

```
...
 <title>serverclasses</title>
 <id>https://localhost:8089/services/deployment/server/serverclasses</id>
 <updated>2013-10-09T08:54:09-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/serverclasses/_new" rel="create"/>
 <link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>sc_apps_shadow</title>
   <id>https://localhost:8089/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow</id>
   <updated>2013-10-09T08:54:09-07:00</updated>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="list"/>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="edit"/>
   <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="remove"/>
   <link href="/servicesNS/nobody/search/deployment/serverclasses/sc_apps_shadow/applications"
rel="applications"/>
   <link href="/servicesNS/nobody/search/deployment/serverclasses/sc_apps_shadow/clients" rel="clients"/>
   <link href="/servicesNS/nobody/search/deployment/serverclasses/sc_apps_shadow/reload" rel="reload"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="blacklist-size">0</s:key>
       <s:key name="currentDownloads">0</s:key>
       ... eai:acl node elided ...
       <s:key name="loadTime">1381334049</s:key>
       <s:key name="machineTypesFilter"></s:key>
       <s:key name="repositoryList">
         <s:dict>
           <s:key name="tmp"/>
           <s:key name="wma-app-test2"/>
           <s:key name="wma-app3"/>
           <s:key name="wma-app_test1"/>
         </s:dict>
       </s:key>
       <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
       <s:key name="restartSplunkd">0</s:key>
       <s:key name="stateOnClient">enabled</s:key>
       <s:key name="whitelist-size">0</s:key>
     </s:dict>
   </content>
 </entry>
```

deployment/server/serverclasses/{name}

`https://<host>:<mPort>/services/deployment/server/serverclasses/{name}`

Manage the `{name}` serverclass.

DELETE

Remove the specfied server class from this deployment server.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/deployment/server/serverclasses/sc_apps_shadow
```

XML Response

```
...
 <title>serverclasses</title>
 <id>https://localhost:8089/services/deployment/server/serverclasses</id>
 <updated>2013-10-09T09:13:27-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/serverclasses/_new" rel="create"/>
 <link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>sc_apps_wma</title>
   <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma</id>
   <updated>2013-10-09T09:13:27-07:00</updated>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="list"/>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="edit"/>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="remove"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_apps_wma/applications"
rel="applications"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_apps_wma/clients" rel="clients"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_apps_wma/reload" rel="reload"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="blacklist-size">0</s:key>
       <s:key name="currentDownloads">0</s:key>
       ... eai:acl node elided ...
       <s:key name="loadTime">1381335207</s:key>
       <s:key name="machineTypesFilter"></s:key>
       <s:key name="repositoryList">
         <s:dict>
           <s:key name="tmp"/>
           <s:key name="wma-app-test2"/>
           <s:key name="wma-app3"/>
           <s:key name="wma-app_test1"/>
         </s:dict>
       </s:key>
       <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
       <s:key name="restartSplunkd">0</s:key>
       <s:key name="stateOnClient">enabled</s:key>
       <s:key name="whitelist-size">1</s:key>
       <s:key name="whitelist.0">Ombra*</s:key>
     </s:dict>
   </content>
 </entry>
 ... elided ...
```

GET

List information about the named server class.

Request parameters

Name	Type	Default	Description
clientId	String		GUID of a deployment client that is a member of the named server class. Lists information about the named server class with respect to this client.
hasDeploymentError	Boolean		Indicates whether to only list server classes that have a deployment error.

Returned values

Name	Description
blacklist-size	Specifies the size of the blacklist for the named server class.
clientId	ID of deployment client for this server class.
currentDownloads	The number of entires in the blacklist for this serverclass.
hasDeploymentError	Indicates whether the serverclass has at least one deployment error.
loadTime	The time, in epoch seconds, this serverclass was loaded.
machineTypesFilter	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
repositoryList	List of applications stored at the location specified by repositoryLocation.
repositoryLocation	The location on the deployment server to store the content that is to be deployed for this server class.
restartSplunkWeb	Indicates whether to restart Splunk Web.
restartSplunkd	Indicates whether to restart splunkd.
stateOnClient	Indicates whether this server class is enabled or disabled.
whitelist-size	Specifies the number of entries in the whitelist for this server class.
whitelist.0	List of servers for whitelist.0 for this server class.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses/sc_mach_type
```

XML Response

```
...
 <title>serverclasses</title>
 <id>https://localhost:8089/services/deployment/server/serverclasses</id>
 <updated>2013-08-04T19:19:34-07:00</updated>
 <generator build="172889" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/serverclasses/_new" rel="create"/>
 <link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>sc_mach_type</title>
   <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type</id>
   <updated>2013-08-04T19:19:34-07:00</updated>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="list"/>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="edit"/>
   <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="remove"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_mach_type/applications"
rel="applications"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_mach_type/clients" rel="clients"/>
   <link href="/servicesNS/nobody/system/deployment/serverclasses/sc_mach_type/reload" rel="reload"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="blacklist-size">0</s:key>
       <s:key name="currentDownloads">0</s:key>
       ... eai:acl node elided ...
       <s:key name="eai:attributes">... elided ...</s:key>
       <s:key name="loadTime">1375467593</s:key>
       <s:key name="machineTypesFilter">linux-x86_64,</s:key>
       <s:key name="repositoryList">
         <s:dict>
           <s:key name="wma-app2"/>
           <s:key name="wma-app1"/>
         </s:dict>
       </s:key>
       <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
       <s:key name="restartSplunkWeb">0</s:key>
       <s:key name="restartSplunkd">0</s:key>
       <s:key name="stateOnClient">enabled</s:key>
       <s:key name="whitelist-size">1</s:key>
       <s:key name="whitelist.0">Ombra*</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Update the named server class.

Request parameters

Name	Type	Default	Description
*blacklist.**	String		List of hosts to exclude for this server class.

Name	Type	Default	Description
			For each blacklist, replace * with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.
continueMatching	Boolen		Controls how configuration is layered across classes and server-specific settings. If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used. Matching is done in the order that server classes are defined. Defaults to true. A serverClass can override this property and stop the matching.
filterType	Enum		Valid values: (whitelist | blacklist) Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters. The whitelist setting indicates a filtering strategy that pulls in a subset: • Items are not considered to match the server class by default. • Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class. • Items that match any blacklist entry are not considered to match the server class, regardless of whitelist. The blacklist setting indicates a filtering strategy that rules out a subset: • Items are considered to match the server class by default. • Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class. • Items that match any whitelist entry are considered to match the server class. More briefly: whitelist: default no-match -> whitelists enable -> blacklists disable blacklist: default match -> blacklists disable-> whitelists enable If you specify whitelist at the global level, and then specify blacklist for an individual server class, the setting becomes blacklist for that server class, and you have to provide another filter in that server class definition to replace the one you overrode.
machineTypesFilter	String		Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters. Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included. Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter. The patterns are PCRE regular expressions, with the following aids for easier entry:

Name	Type	Default	Description
			- You can specify '.' to mean '\\.' - You can specify '*' to mean '.*' - Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.
repositoryLocation	String		The location on the deployment server to store the content that is to be deployed for this server class. For example: $SPLUNK_HOME/etc/deployment-apps
restartSplunkWeb	Boolean		Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated. Defaults to false
restartSplunkd	Boolean		Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated. Defaults to false
stateOnClient	Enum		Valid values are (enabled | disabled | noop). - *enabled*: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server. - *disabled*: Sets the application state to disabled on the client, regardless of state on the deployment server. - *noop*: The state on the client is the same as on the deployment server.
targetRepositoryLocation	String		The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used. That is, defaults to: $SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk instance Useful only with complex (for example, tiered) deployment strategies.
tmpFolder	String		Working folder used by deployment server. Defaults to $SPLUNK_HOME/var/run/tmp
*whitelist.**	String		List of hosts to accept for this server class. For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses/sc_apps_ombra -d
stateOnClient=noop
```

XML Response

```
 <title>serverclasses</title>
 <id>https://localhost:8089/services/deployment/server/serverclasses</id>
 <updated>2013-08-10T13:24:16-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/deployment/server/serverclasses/_new" rel="create"/>
 <link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>sc_apps_ombra</title>
   <id>https://localhost:8089/services/deployment/server/serverclasses/sc_apps_ombra</id>
   <updated>2013-08-10T13:24:16-07:00</updated>
   <link href="/services/deployment/server/serverclasses/sc_apps_ombra" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/deployment/server/serverclasses/sc_apps_ombra" rel="list"/>
   <link href="/services/deployment/server/serverclasses/sc_apps_ombra" rel="edit"/>
   <link href="/services/deployment/server/serverclasses/sc_apps_ombra" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       ... opensearch nodes elided ...
     </s:dict>
   </content>
 </entry>
```

search/distributed/bundle/replication/config

`https://<host>:<mPort>/services/search/distributed/bundle/replication/config`
Provides information on knowledge bundle replication configuration on a search head.

Authentication and Authorization
Requires the `search` capability.

Usage details
See Troubleshoot knowledge bundle replication in *Distributed Search*.

GET

List knowledge bundle replication configuration settings.

Request parameters
None

Returned values

Name	Description
concerningReplicatedFileSize	A warning will be logged if the bundle lookup size exceeds this value
connectionTimeout	Timeout value for establishing connection between search head and indexer
maxBundleSize	Maximum allowable bundle size
receiveTimeout	Timeout value for receiving data between search head and indexer
replicationPeriod	Period during which the replicationThread checks whether bundle replication is required
replicationPolicy	Bundle replication policy in use
sendTimeout	Timeout value for sending data between search head and indexer
statusQueueSize	Size of the cycles maintained in memory and available through the cycles endpoint

Example request and response

XML Request

```
curl -k -u admin:changeme https://ronnie:8089/services/search/distributed/bundle/replication/config
```

XML Response

```
 <feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bundle-replication-config</title>
  <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/config</id>
  <updated>2019-08-23T16:26:22-07:00</updated>
  <generator build="9f02da632403" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>bundleReplicationConfig</title>
    <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/config
/bundleReplicationConfig</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/search/distributed/bundle/replication/config/bundleReplicationConfig"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/distributed/bundle/replication/config/bundleReplicationConfig" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="concerningReplicatedFileSize">524288000</s:key>
        <s:key name="connectionTimeout">60</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>power</s:item>
                    <s:item>splunk-system-role</s:item>
                    <s:item>user</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="maxBundleSize">2147483648</s:key>
        <s:key name="receiveTimeout">60</s:key>
        <s:key name="replicationPeriod">60</s:key>
        <s:key name="replicationPolicy">classic</s:key>
        <s:key name="replicationThreads">9</s:key>
        <s:key name="sendTimeout">60</s:key>
        <s:key name="statusQueueSize">5</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/distributed/bundle/replication/cycles

`https://<host>:<mPort>/services/search/distributed/bundle/replication/cycles`
Provides information and status for knowledge bundle replication cycles on a search head.

Authentication and Authorization

Requires the `search` capability.

Usage details

See Troubleshoot knowledge bundle replication in *Distributed Search*.

GET

List information and status for knowledge bundle replication cycles..

Request parameters

Name	Type	Description
latest	Boolean	Optional. If set to `true`, information about only the latest cycle is returned.

Returned values

Name	Description
bundle_id	Knowledge bundle unique identifier composed of `hostname-creation_time`
current_bundle	Path to active knowledge bundle on disk
current_repl_start_time	Start time of current replication cycle
cycle_id	Bundle replication cycle unique identifier
delta_path	Path to the delta knowledge bundle on disk, if a delta was created
is_repl_in_progress	Boolean to indicate whether the replication cycle is in progress or completed
peers_status	Entry for each peer with `peer_name` and replication state for each peer
replicationPolicy	Bundle replication policy in use

Example request and response

XML Request

```
curl -k -u admin:changeme
https://ronnie:8089/services/search/distributed/bundle/replication/cycles?latest=true
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bundle-replication-cycles</title>
  <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/cycles</id>
  <updated>2019-08-23T16:32:20-07:00</updated>
  <generator build="9f02da632403" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>80CC124B-2D46-44A7-95C2-A92ECC32C050</title>
    <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/cycles/80CC124B-2D46
-44A7-95C2-A92ECC32C050</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/search/distributed/bundle/replication/cycles/80CC124B-2D46-44A7-95C2-A92ECC32C050"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/distributed/bundle/replication/cycles/80CC124B-2D46-44A7-95C2-A92ECC32C050"
rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="bundle_id">qa-centos7x64-056-1566601784</s:key>
        <s:key
name="current_bundle">/root/splunk_install/var/run/qa-centos7x64-056-1566601784.bundle</s:key>
        <s:key name="current_repl_start_time">1566602286</s:key>
        <s:key name="cycle_id">80CC124B-2D46-44A7-95C2-A92ECC32C050</s:key>
        <s:key
```

```
name="delta_path">/root/splunk_install/var/run/qa-centos7x64-056-1566601708-1566601784.delta</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>power</s:item>
                    <s:item>splunk-system-role</s:item>
                    <s:item>user</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="is_repl_in_progress">0</s:key>
        <s:key name="peers_status">
          <s:dict>
            <s:key name="https://10.140.126.37:8089">
              <s:dict>
                <s:key name="classic_replication_state">succeeded</s:key>
                <s:key name="peer_name">https://10.140.126.37:8089</s:key>
              </s:dict>
            </s:key>
            <s:key name="https://10.140.127.113:8089">
              <s:dict>
                <s:key name="classic_replication_state">succeeded</s:key>
                <s:key name="peer_name">https://10.140.127.113:8089</s:key>
              </s:dict>
            </s:key>
            <s:key name="https://10.140.127.79:8089">
              <s:dict>
                <s:key name="classic_replication_state">succeeded</s:key>
                <s:key name="peer_name">https://10.140.127.79:8089</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="replicationPolicy">classic</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/distributed/bundle-replication-files

`https://<host>:<mPort>/services/search/distributed/bundle-replication-files`
Access information for the most recent distributed search bundle.

GET

List distributed search bundle replication files.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
checksum	Common checksum for entities in the bundle.
filename	Bundle file name
location	Bundle file path
size	Bundle size, in bytes
timestamp	Bundle creation timestamp.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/distributed/bundle-replication-files
```

XML Response

```
...
 <title>search-head-bundles</title>
 <id>https://localhost:8089/services/search/distributed/bundle-replication-files</id>
 <updated>2013-10-09T09:42:51-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>13134207368020721783</title>
   <id>https://localhost:8089/services/search/distributed/bundle-replication-files/13134207368020721783</id>
   <updated>2013-10-09T09:42:51-07:00</updated>
   <link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="checksum">13134207368020721783</s:key>
       ... eai:acl node elided ...
       <s:key name="filename">localhost-1381336958.bundle</s:key>
       <s:key name="location">/opt/cluster/peer1/splunk/var/run/localhost-1381336958.bundle</s:key>
       <s:key name="timestamp">1381336958</s:key>
     </s:dict>
   </content>
 </entry>
```

search/distributed/bundle-replication-files/{name}

`https://<host>:<mPort>/services/search/distributed/bundle-replication-files/{name}`
Get `{name}` bundle replication file information.

GET

List information about the specified bundle replication file. For `{name}`, specify the checksum for the file.

Request parameters

Name	Type	Default	Description
force_list_all	Boolean		Indicates whether to force a listing of the file.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/search/distributed/bundle-replication-files/13134207368020721783
```

XML Response

```
...
 <title>search-head-bundles</title>
 <id>https://localhost:8089/services/search/distributed/bundle-replication-files</id>
 <updated>2013-10-09T10:07:17-07:00</updated>
 <generator build="176231" version="6.0"/>
 <author>
   <name>Splunk</name>
```

```
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>13134207368020721783</title>
  <id>https://localhost:8089/services/search/distributed/bundle-replication-files/13134207368020721783</id>
  <updated>2013-10-09T10:07:17-07:00</updated>
  <link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="checksum">13134207368020721783</s:key>
      ... eai:acl node elided ...
      <s:key name="eai:attributes">... elided ...</s:key>
      <s:key name="filename">localhost-1381336958.bundle</s:key>
      <s:key name="location">/opt/cluster/peer1/splunk/var/run/localhost-1381336958.bundle</s:key>
      <s:key name="timestamp">1381336958</s:key>
    </s:dict>
  </content>
</entry>
```

search/distributed/config

`https://<host>:<mPort>/services/search/distributed/config`

Provides access to the Splunk Enterprise distributed search options. This option is not for adding search peers.

GET

Lists the configuration options for the distributed search system.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
autoAddServers	[Deprecated]
blacklistNames	List of filenames that match the blacklist pattern, and are not replicated.
blacklistURLs	List of URLs that are blacklisted, and thus is not replicated.
checkTimedOutServersFrequency	Rechecks servers at the specified frequency (in seconds). If this is set to 0, then no recheck occurs. Defaults to 60. This attribute is ONLY relevant if *removeTimedOutServers* is set to `true`. If *removeTimedOutServers* is `false`, this attribute is ignored.

Name	Description
connectionTimeout	Connection timeout.
disabled	Indicates if the distributed search is disabled.
dist_search_enabled	Indicates if the distributed search is enabled.
heartbeatFrequency	[Deprecated]
heartbeatMcastAddr	[Deprecated]
heartbeatPort	[Deprecated]
receiveTimeout	Amount of time in seconds to use as a timeout while trying to read/receive data from a search peer.
removedTimedOutServers	If true, removes a server connection that cannot be made within serverTimeout. If false, every call to that server attempts to connect. This may result in a slow user interface.
sendTimeout	Send timeout.
serverTimeout	[Deprecated] Refer to *connectionTimeout*, *sendTimeout*, and *receiveTimeout*.
servers	The initial list of servers. If operating completely in autoAddServers mode (discovering all servers), there is no need to list any servers here.
shareBundles	Indicates whether this server uses bundle replication to share search time configuration with search peers. If set to false, the search head assumes that the search peers can access the correct bundles using an NFS share and have correctly configured the options listed under: "SEARCH HEAD BUNDLE MOUNTING OPTIONS."
skipOurselves	[Deprecated]
statusTimeout	Set connection timeout when gathering a search peer's basic info (/services/server/info). Read/write timeouts are automatically set to twice this value.
ttl	[Deprecated]

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/distributed/config
```

XML Response

```
...
 <title>distsearch-setup</title>
 <id>https://localhost:8089/services/search/distributed/config</id>
 <updated>2011-07-10T23:21:51-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
```

```
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>distributedSearch</title>
  <id>https://localhost:8089/services/search/distributed/config/distributedSearch</id>
  <updated>2011-07-10T23:21:51-07:00</updated>
  <link href="/services/search/distributed/config/distributedSearch" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/config/distributedSearch" rel="list"/>
  <link href="/services/search/distributed/config/distributedSearch" rel="edit"/>
  <link href="/services/search/distributed/config/distributedSearch" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="autoAddServers">0</s:key>
      <s:key name="blacklistNames"/>
      <s:key name="blacklistURLs"/>
      <s:key name="checkTimedOutServersFrequency">60</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="dist_search_enabled">1</s:key>
      ... eai:acl node elided ...
      <s:key name="heartbeatFrequency">0</s:key>
      <s:key name="heartbeatMcastAddr">224.0.0.37</s:key>
      <s:key name="heartbeatPort">8888</s:key>
      <s:key name="removedTimedOutServers">0</s:key>
      <s:key name="serverTimeout">10</s:key>
      <s:key name="servers"/>
      <s:key name="shareBundles">1</s:key>
      <s:key name="skipOurselves">0</s:key>
      <s:key name="statusTimeout">10</s:key>
      <s:key name="ttl">1</s:key>
    </s:dict>
  </content>
</entry>
```

search/distributed/peers

`https://<host>:<mPort>/services/search/distributed/peers`

Provides distributed peer server management. A search peer is defined as a Splunk server to which another Splunk server distributes searches. The Splunk server where the search request originates is referred to as the search head.

GET

Get configured search peers to which this search head is configured to distribute searches. This includes configured but disabled search peers.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
build	The Splunk build number for this peer.
bundle_versions	The IDs of the bundles (of this search head) that the peer has. The IDs are sorted from latest to earliest.
disabled	Indicates if the peer is disabled.
guid	GUID of the peer.
is_https	Inidcates if the management port is using SSL.
licenseSignature	The license signature.
peerName	The Splunk server name of the peer.
peerType	Specifies whether the peer is configured or discovered.
replicationStatus	The status of bundle replication to this peer. Can be any of the following values: Initial In progress Failed Successful Mounted
status	The status of the peer. Can be one of the following values: Up Down Blacklisted Not a Splunk server Free Splunk server Authentication Failed Duplicate License Duplicate Servername Inconsistent bundles
status_details	Details of any errors encountered in the last heartbeat period.
version	The Splunk software version string this peer is running.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/distributed/peers
```

XML Response

```
...
 <title>distsearch-peer</title>
```

```
<id>https://localhost:8089/services/search/distributed/peers</id>
<updated>2011-07-11T18:21:48-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/search/distributed/peers/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>tiny:8090</title>
  <id>https://localhost:8089/services/search/distributed/peers/tiny%3A8090</id>
  <updated>2011-07-11T18:21:48-07:00</updated>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="list"/>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="edit"/>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="remove"/>
  <link href="/services/search/distributed/peers/tiny%3A8090/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="build"/>
      <s:key name="bundle_versions">
        <s:list/>
      </s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl node elided ...
      <s:key name="guid"/>
      <s:key name="is_https">1</s:key>
      <s:key name="licenseSignature"/>
      <s:key name="peerName">tiny:8090</s:key>
      <s:key name="peerType">configured</s:key>
      <s:key name="replicationStatus">Initial</s:key>
      <s:key name="status">Down</s:key>
      <s:key name="version"/>
    </s:dict>
  </content>
</entry>
```

POST

Add a new distributed search peer.

Usage details

The distributed search must first be enabled using the search/distributed/config endpoint.

Request parameters

Name	Type	Required	Default	Description
name	String			The name of the search peer. Defined as hostname:port, where port is the management port.
remotePassword	String			The password of the remote user.

Name	Type	Required	Default	Description
remoteUsername	String			The username of a user with admin privileges in the search peer server. This is used to exchange certificates.

HTTP response codes

Status Code	Description
201	Created successfully.
400	Request error. See response body for details.
401	Authentication failure: must pass valid credentials with request.
402	The Splunk license in use has disabled this feature.
403	Insufficient permissions to create specified resource.
409	Request error: this operation is invalid for this item. See response body for details.
500	Internal server error. See response body for details.
503	This feature has been disabled in Splunk configuration files.

Returned values

No values returned for this request.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/distributed/peers -d name=MrT:8092 -d
remoteUsername=admin -d remotePassword=mypass
```

XML Response

```
.
.
.
 <title>distsearch-peer</title>
 <id>https://localhost:8089/services/search/distributed/peers</id>
 <updated>2011-07-11T18:22:00-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/search/distributed/peers/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

search/distributed/peers/{name}

```
https://<host>:<mPort>/services/search/distributed/peers
```

Manage distributed peer servers. A search peer is defined as a Splunk server to which another Splunk server distributes searches. The Splunk server where the search request originates is referred to as the search head.

POST

Update a peer server.

Usage details

The distributed search must first be enabled using the search/distributed/config endpoint.

Request parameters

Name	Type	Required	Default	Description
remotePassword	String			The password of the remote user.
remoteUsername	String			The username of a user with admin privileges in the search peer server. This is used to exchange certificates.

Returned values

See example.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/distributed/peers/MrT:8092  -d
remoteUsername=admin -d remotePassword=mypass
```

XML Response

```
.
.
.
 <title>distsearch-peer</title>
 <id>https://localhost:8089/services/search/distributed/peers</id>
 <updated>2011-07-11T18:22:00-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/search/distributed/peers/_new" rel="create"/>
```

```
... opensearch nodes elided ...
<s:messages/>
```

Federated Search endpoints

Federated search endpoint descriptions

Use the federated search REST API endpoints to create, update, and delete definitions for federated providers and federated indexes for Federated Search for Splunk and Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform.

See Overview of the federated search options for the Splunk platform in *Federated Search*.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication are required for access to endpoints and REST operations.

Splunk users must have role or capability-based authorization to use REST endpoints, and must have the admin_all_objects and edit_indexes **capabilities** to use the federated search endpoints detailed in this topic.

Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings > Access controls > Users**. To determine the capabilities assigned to a role, select **Settings > Access controls > Roles**.

Splunk Cloud Platform URL for REST API access

Splunk Cloud Platform has a different host and management port syntax than Splunk Enterprise. Paid subscribers to the Splunk Cloud Platform service use the following URL to access REST API resources:

```
https://<deployment-name>.splunkcloud.com:8089
```

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

---

data/federated/settings/general

```
https://<host>:<mPort>/services/data/federated/settings/general
```

Use this endpoint to review the general settings for your Splunk platform deployment implementation of Federated Search for Splunk and change those settings as necessary. For an overview of Federated Search for Splunk, see About Federated Search for Splunk in *Federated Search*.

> The settings that this endpoint governs do not apply to Federated Search for Amazon S3.

Authentication and authorization

Usage of the GET and POST operations for this endpoint is restricted to roles that have the admin_all_objects **capability**.

GET

Provides the current general federated search settings for your Splunk platform deployment.

Request parameters

None specific to this method. This method can use pagination and filtering parameters.

Returned values

Name	Description
disabled	Specifies whether federated search functionality is turned on for your Splunk platform deployment. If `disabled = false`, federated search functionality is turned on for your deployment. If `disabled = true`, federated search functionality is turned off for your deployment. Defaults to `false`.
transparent_mode	Specifies whether transparent mode federated search functionality is turned on for your Splunk platform deployment. If set to `true`, transparent mode is turned on, which means federated search users on your deployment can run federated searches over transparent mode federated providers as well as standard mode federated providers. If set to `false`, transparent mode is turned off, which means federated search users on your deployment can run federated searches only over standard mode federated providers. Defaults to `true`.
controlCommandsFeatureEnabled	Specifies whether a federated search head can send a federated search action, such as a search cancellation, to federated providers. Does not support search pause. Defaults to `true`.
controlCommandsMaxThreads	The maximum number of threads that can run a federated search action, such as a search cancellation, from a federated search head, on federated providers. Does not support search pause. Defaults to `5`.
controlCommandsMaxTimeThreshold	The maximum number of seconds that a federated search head waits for the completion of a federated search action such as a search cancellation. Does not support search pause. Defaults to `5`.
heartbeatEnabled	Specifies whether the federated search heartbeat mechanism is running. The heartbeat mechanism monitors the remote federated providers. If it detects problems with the federated providers the heartbeat mechanism can tell you what is wrong and take actions. Defaults to `true`.
max_preview_generation_duration	The maximum amount of time, in seconds, that the search head can spend to generate search result previews. When this limit is reached by a federated search, preview preview generation is halted, but the search continues gathering results until it completes and displays the final result set. A setting of `0` means that the preview generation duration of federated searches is unlimited. Defaults to `0`.
needs_consent	When set to `true`, `needs_consent` causes a checkbox to appear in the UI for federated provider definitions and index assignment to roles. This checkbox requires that users acknowledge that federated providers and federated index permissions can be set up in a manner detrimental to regulatory compliance. When set to `false`, `needs_consent` hides this checkbox. Defaults to `true`.
proxyBundlesTTL	Specifies the time to live in seconds of a proxy bundle on the remote search head after the last time it was used by a search. Defaults to `172800` seconds, or 2 days.

Name	Description
remoteEventsDownloadRetryCountMax	When you run a verbose-mode federated search, the federated search head downloads events from the federated provider. This setting provides the maximum number of event download retries that the federated search head can make before it reports an event download failure. Related to `remoteEventsDownloadRetryTimeoutMs`. Defaults to `20` event download retries.
remoteEventsDownloadRetryTimeoutMs	When you run a verbose-mode federated search, the federated search head downloads events from the federated provider. This setting provides the interval, in milliseconds, between retries of a failed event download from a federated provider. Related to `remoteEventsDownloadRetryCountMax`. Defaults to `1000`.
verbose_mode	Specifies whether federated searches can be run in verbose mode. A setting of `false` restricts the ability of federated searches to run in verbose mode, while allowing federated searches to run in fast or smart mode. In transparent mode, a setting of `false` means that Splunk software runs only the local portion of a verbose mode federated search. In standard mode, a setting of `false` terminates verbose mode federated searches without displaying their results. Defaults to `true`.

Example request and response

Return the general federated search settings for your Splunk platform deployment. The XML response shows an example of returned federated search settings.

XML Request

```
curl -k -u admin:changeme -X GET https://localhost:8089/services/data/federated/settings/general
```

XML response

```
...
  <entry>
    <title>general</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/settings/general</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/settings/general" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/settings/general" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/settings/general/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/settings/general" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/settings/general/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="controlCommandsFeatureEnabled">1</s:key>
        <s:key name="controlCommandsMaxThreads">5</s:key>
        <s:key name="controlCommandsMaxTimeThreshold">5</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
```

```
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>controlCommandsFeatureEnabled</s:item>
                <s:item>controlCommandsMaxThreads</s:item>
                <s:item>controlCommandsMaxTimeThreshold</s:item>
                <s:item>heartbeatEnabled</s:item>
                <s:item>needs_consent</s:item>
                <s:item>proxyBundlesTTL</s:item>
                <s:item>verbose_mode</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>.*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="max_preview_generation_duration">0<s:key>
        <s:key name="needs_consent">1</s:key>
        <s:key name="proxyBundlesTTL">172800</s:key>
        <s:key name="remoteEventsDownloadRetryCountMax">20</s:key>
        <s:key name="remoteEventsDownloadRetryTimeoutMs">1000</s:key>
        <s:key name="transparent_mode">1</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Updates general federated search settings. Can be used to turn federated search functionality on or off for a Splunk platform deployment.

Request parameters

Name	Type	Description
disabled	Boolean	When set to `false`, `disabled` specifies that federated search functionality is turned on for your Splunk platform deployment. When set to `true`, `disabled` specifies that federated search functionality is turned off for your Splunk platform deployment.

Name	Type	Description
		Defaults to `false`.
transparent_mode	Boolean	When set to `true`, `transparent_mode` specifies that transparent mode federated search functionality is turned on for your Splunk platform deployment, which means that federated search users on your deployment can run federated searches over transparent mode federated providers as well as standard mode federated providers. When set to `false`, `transparent_mode` specifies that transparent mode federated search functionality is turned off for your Splunk platform deployment, which means that federated search users on your deployment can run federated searches only over standard mode federated providers. Defaults to `true`. **Note:** After turning on or off transparent mode, you must call _reload by running the following HTTP POST request; otherwise the change won't take effect: curl -k -u admin:changeme -X POST https://localhost:management-port/services/configs/conf-federated/_reload
controlCommandsFeatureEnabled	Boolean	Specifies whether a federated search head can send a federated search action, such as a search cancellation, to federated providers. Does not support search pause. Defaults to `true`. Change this setting only when instructed to do so by Splunk Support.
controlCommandsMaxThreads	Number	The maximum number of threads that can run a federated search action, such as a search cancellation, from a federated search head, on federated providers. Does not support search pause. Defaults to `5`. Change this setting only when instructed to do so by Splunk Support.
controlCommandsMaxTimeThreshold	Number	The maximum number of seconds that a federated search head waits for the completion of a federated search action such as a search cancellation. Does not support search pause. Defaults to `5`. Change this setting only when instructed to do so by Splunk Support.
heartbeatEnabled	Boolean	Specifies whether the federated search heartbeat mechanism is running. The heartbeat mechanism monitors the remote federated providers. If it detects problems with the federated providers the heartbeat mechanism can tell you what is wrong and take actions. Defaults to `true`. Change this setting only when instructed to do so by Splunk Support.
max_preview_generation_duration	Number	The maximum amount of time, in seconds, that the search head can spend to generate search result previews. When this limit is reached by a federated search, preview preview generation is halted, but the search continues gathering results until it completes and displays the final result set. A setting of `0` means that the preview generation duration of federated searches is unlimited. Defaults to `0`. Change the value of this setting to a number above zero if you find that your federated searches are terminated because their preview generation duration exceeds a timeout set by another component in your network, such as an elastic load balancer (ELB). For example, if you have an ELB that times out your searches after 60 seconds, set `max_preview_generation_duration` to `55`.
needs_consent	Boolean	When set to `true`, `needs_consent` causes a checkbox to appear in the UI for federated provider definitions and index assignment to roles. This checkbox requires that users acknowledge that federated providers and federated index permissions can be set up in a manner detrimental to regulatory compliance. When set to `false`, `needs_consent` hides this checkbox. Defaults to `true`.

Name	Type	Description
		Change this setting only when instructed to do so by Splunk Support.
proxyBundlesTTL	Number	Specifies the time to live in seconds of a proxy bundle on the remote search head after the last time it was used by a search. Defaults to `172800` seconds, or 2 days. Change this setting only when instructed to do so by Splunk Support.
remoteEventsDownloadRetryCountMax	Number	When you run a verbose-mode federated search, the federated search head downloads events from the federated provider. This setting provides the maximum number of event download retries that the federated search head can make before it reports an event download failure. Related to `remoteEventsDownloadRetryTimeoutMs`. Defaults to `20` event download retries. Change this setting only when instructed to do so by Splunk Support.
remoteEventsDownloadRetryTimeoutMs	Number	When you run a verbose-mode federated search, the federated search head downloads events from the federated provider. This setting provides the interval, in milliseconds, between retries of a failed event download from a federated provider. Related to `remoteEventsDownloadRetryCountMax`. Defaults to `1000`. Change this setting only when instructed to do so by Splunk Support.
verbose_mode	Boolean	Specifies whether federated searches can be run in verbose mode. A setting of `false` restricts the ability of federated searches to run in verbose mode, while allowing federated searches to run in fast or smart mode. In transparent mode, a setting of `false` means that Splunk software runs only the local portion of a verbose mode federated search. In standard mode, a setting of `false` terminates verbose mode federated searches without displaying their results. Defaults to `true`. Change this setting only when instructed to do so by Splunk Support.

Returned values

Name	Description
disabled	Specifies whether federated search functionality is turned on for your Splunk platform deployment. If `disabled = false`, federated search functionality is turned on for your deployment. If `disabled = true`, federated search functionality is turned off for your deployment. Defaults to `false`.
transparent_mode	Specifies whether transparent mode federated search functionality is turned on for your Splunk platform deployment. If set to `true`, transparent mode is turned on, which means federated search users on your deployment can run federated searches over transparent mode federated providers as well as standard mode federated providers. If set to `false`, transparent mode is turned off, which means federated search users on your deployment can run federated searches only over standard mode federated providers. Defaults to `true`.
controlCommandsFeatureEnabled	Specifies whether a federated search head can send a federated search action, such as a search cancellation, to federated providers. Does not support search pause. Defaults to `true`.
controlCommandsMaxThreads	The maximum number of threads that can run a federated search action, such as a search cancellation, from a federated search head, on federated providers. Does not support search pause. Defaults to `5`.

Name	Description
controlCommandsMaxTimeThreshold	The maximum number of seconds that a federated search head waits for the completion of a federated search action such as a search cancellation. Does not support search pause. Defaults to `5`.
heartbeatEnabled	Specifies whether the federated search heartbeat mechanism is running. The heartbeat mechanism monitors the remote federated providers. If it detects problems with the federated providers the heartbeat mechanism can tell you what is wrong and take actions. Defaults to `true`.
max_preview_generation_duration	The maximum amount of time, in seconds, that the search head can spend to generate search result previews. When this limit is reached by a federated search, preview preview generation is halted, but the search continues gathering results until it completes and displays the final result set. A setting of `0` means that the preview generation duration of federated searches is unlimited. Defaults to `0`.
needs_consent	When set to `true`, `needs_consent` causes a checkbox to appear in the UI for federated provider definitions and index assignment to roles. This checkbox requires that users acknowledge that federated providers and federated index permissions can be set up in a manner detrimental to regulatory compliance. When set to `false`, `needs_consent` hides this checkbox. Defaults to `true`.
proxyBundlesTTL	Specifies the time to live in seconds of a proxy bundle on the remote search head after the last time it was used by a search. Defaults to `172800` seconds, or 2 days.
remoteEventsDownloadRetryCountMax	When you run a verbose-mode federated search, the federated search head downloads events from the federated provider. This setting provides the maximum number of event download retries that the federated search head can make before it reports an event download failure. Related to `remoteEventsDownloadRetryTimeoutMs`. Defaults to `20` event download retries.
remoteEventsDownloadRetryTimeoutMs	When you run a verbose-mode federated search, the federated search head downloads events from the federated provider. This setting provides the interval, in milliseconds, between retries of a failed event download from a federated provider. Related to `remoteEventsDownloadRetryCountMax`. Defaults to `1000`.
verbose_mode	Specifies whether federated searches can be run in verbose mode. A setting of `false` restricts the ability of federated searches to run in verbose mode, while allowing federated searches to run in fast or smart mode. In transparent mode, a setting of `false` means that Splunk software runs only the local portion of a verbose mode federated search. In standard mode, a setting of `false` terminates verbose mode federated searches without displaying their results. Defaults to `true`.

Example request and response

Turn off transparent mode federated search for this Splunk platform deployment.

XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/data/federated/settings/general -d
transparent_mode=false
```

After turning on or off transparent mode, you must call _reload by running the following HTTP POST request; otherwise the change won't take effect: curl -k -u admin:changeme -X POST https://localhost:8089/services/configs/conf-federated/_reload

XML response

```
...
<entry>
    <title>general</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/settings/general</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/settings/general" rel="alternate"/>
    <author>
```

```
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/data/federated/settings/general" rel="list"/>
<link href="/servicesNS/nobody/system/data/federated/settings/general/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/system/data/federated/settings/general" rel="edit"/>
<link href="/servicesNS/nobody/system/data/federated/settings/general/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:key name="controlCommandsFeatureEnabled">1</s:key>
    <s:key name="controlCommandsMaxThreads">5</s:key>
    <s:key name="controlCommandsMaxTimeThreshold">5</s:key>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app">system</s:key>
        <s:key name="can_change_perms">1</s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_share_app">1</s:key>
        <s:key name="can_share_global">1</s:key>
        <s:key name="can_share_user">0</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">1</s:key>
        <s:key name="owner">nobody</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="eai:attributes">
      <s:dict>
        <s:key name="optionalFields">
          <s:list>
            <s:item>controlCommandsFeatureEnabled</s:item>
            <s:item>controlCommandsMaxThreads</s:item>
            <s:item>controlCommandsMaxTimeThreshold</s:item>
            <s:item>heartbeatEnabled</s:item>
            <s:item>needs_consent</s:item>
            <s:item>proxyBundlesTTL</s:item>
            <s:item>verbose_mode</s:item>
          </s:list>
        </s:key>
        <s:key name="requiredFields">
          <s:list/>
        </s:key>
        <s:key name="wildcardFields">
          <s:list>
            <s:item>.*</s:item>
          </s:list>
        </s:key>
```

```
          </s:dict>
        </s:key>
        <s:key name="max_preview_generation_duration">0<s:key>
        <s:key name="needs_consent">1</s:key>
        <s:key name="proxyBundlesTTL">172800</s:key>
        <s:key name="remoteEventsDownloadRetryCountMax">20</s:key>
        <s:key name="remoteEventsDownloadRetryTimeoutMs">1000</s:key>
        <s:key name="transparent_mode">0</s:key>
      </s:dict>
    </content>
  </entry>
```

data/federated/provider

`https://<host>:<mPort>/services/data/federated/provider`

Use this endpoint to get a list of federated providers and post new federated provider definitions. Some of these settings are exclusive to Federated Search for Splunk, while other settings are exclusive to Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform.

> The provider endpoint does not honor user or app context. It always places federated provider stanzas in etc/system/local/federated.conf, no matter which user or app namespace you are currently using.

For more information about defining federated providers for Federated Search for Splunk, see Define a Splunk platform federated provider in *Federated Search*.

For more information about defining federated providers for Federated Search for Amazon S3, see Define an Amazon S3 federated provider in *Federated Search*.

Authentication and authorization

Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects **capability**.

GET

Returns a list of federated providers.

Request parameters

None specific to this method. This method can use pagination and filtering parameters.

Returned values

Name	What providers does this setting apply to?	Description
name	All providers	Specifies the name of the federated provider.
type	All providers	Specifies the federated provider type. If you have a Splunk Enterprise deployment, you can set `type` only to `splunk`, indicating that the provider is for Federated Search for Splunk. If you have a Splunk Cloud Platform deployment, you can set `type` to either `splunk` or `aws_s3`. A `type = aws_s3` setting indicates the provider is

Name	What providers does this setting apply to?	Description
		for Federated Search for Amazon S3. Defaults to `splunk`.
mode	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider runs federated searches in `standard` or `transparent` mode. For a detailed comparison of the standard and transparent modes of federated search, see About Federated Search for Splunk in *Federated Search*. Defaults to `standard`.
appContext	Applies only to Federated Search for Splunk providers	Specifies the Splunk application context for federated searches that are run over standard mode federated providers. The application context ensures that standard mode federated searches using this federated provider are limited to the knowledge objects that are associated with the named application. • If `mode = standard` for this federated provider, `appContext` specifies an the folder name of an app that is installed on the remote search head of the federated provider. • If `mode = transparent` for this federated provider, the federated provider ignores the `appContext` setting when you run federated searches over the provider. Transparent mode federated searches use the application context of the user running the search. Defaults to `search`.
aws_account_id	Applies only to Federated Search for Amazon S3 providers	Specifies a 12-digit Amazon Web Services (AWS) account ID.
aws_glue_tables_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of AWS Glue tables from which Federated Search for Amazon S3 can get metadata and data schemas.
aws_kms_keys_arn_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of the Amazon resource names (ARNs) for the AWS KMS keys that encrypt Amazon S3 data.
aws_region	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Web Services (AWS) region of your Splunk Cloud Platform deployment. This setting is determined automatically by Splunk software.
aws_s3_paths_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of Amazon S3 location paths that you can search with Federated Search for Amazon S3.
database	Applies only to Federated Search for Amazon S3 providers	Specifies the name of the AWS Glue Data Catalog database that contains the AWS Glue Data Catalog tables for the federated provider.
data_catalog	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Resource Name (ARN) for the AWS Glue Data Catalog. The ARN points to an AWS account.
hostPort	Applies only to Federated Search for Splunk providers	Specifies the protocols required to connect to a federated provider. Usually follows this format <Host_Name>:<Service_Port_Number>. In some cases, an IP address is used instead of a host name.
serviceAccount	Applies only to Federated Search for Splunk providers	Specifies the user name for a service account that has been set up on the federated provider for the purpose of facilitating secure federated searches.

Name	What providers does this setting apply to?	Description
useFSHKnowledgeObjects	Applies only to Federated Search for Splunk providers	Specifies whether the remote search head uses its own knowledge objects for federated searches, or if it uses knowledge objects that are bundle-replicated from the federated search head. The federated provider `mode` determines the required setting for `useFSHKnowledgeObjects`. • When the federated provider has `mode=standard`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `0` or `false`, which means that the federated search can use a blend of local and remote knowledge objects. • When the federated provider has `mode=transparent`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `1` or `true`, because transparent mode federated searches can use knowledge objects only from the federated search head.
connectivityStatus	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider established a connection to your local deployment in its last attempt to do so. • When `connectivityStatus=valid`, this federated provider was able to connect to your local deployment. • When `connectivityStatus=invalid`, this federated provider was unable to connect to your local deployment. • When `connectivityStatus=unknown`, the ability of the federated provider to check this connection has been turned off. This setting is for diagnostic purposes only and cannot be set or changed by users.
disabled	All providers	Specifies whether the federated provider is turned on or off. When a federated provider is turned off, the provider cannot return results for federated searches.

Example federated provider request and response

Return a list of all federated providers, regardless of type. The sample XML response returns the details for two Federated Search for Amazon S3 providers and one Federated Search for Splunk provider.

XML request

```
curl -k -u admin:changeme  -X GET https://localhost:8126/services/data/federated/provider
```

XML response

```
...
  <entry>
    <title>provider-test-fss3</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/provider-test-fss3</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3/_reload"
```

```
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="remove"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3/enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">xyz,aaa,abc,cde</s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3:/b1/p1*,s3:/b2/*</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">fss3_db</s:key>
        <s:key name="disabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
<entry>
    <title>test_provider</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/aws_s3_provider </id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">table_1,table_2</s:key>
        <s:key
name="aws_kms_keys_arn_allowlist">arn:aws:kms:us-east-1:123456789012:key/b1e51ce6-210d-49dd-a6a6-7ff950000003<
/s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3://bucket1,s3://bucket2/folder2/</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">database_1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
<entry>
    <title>splunk2splunk_provider_1</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1" rel="remove"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/splunk2splunk_provider_1/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="appContext">search</s:key>
        <s:key name="connectivityStatus">invalid</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="hostPort">buttercupgames.splunkcloud.com:8088</s:key>
        <s:key name="mode">standard</s:key>
        <s:key name="serviceAccount">fedsearch-account</s:key>
        <s:key name="type">splunk</s:key>
        <s:key name="useFSHKnowledgeObjects">0</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

Example Federated Search for Amazon S3 request and response

Return a list of all Federated Search for Amazon S3 federated providers.

XML request

```
curl -k -u admin:changeme --request -X GET https://localhost:8089/services/data/federated/provider -d
type=aws_s3
```

XML response

```
...
<entry>
    <title>provider-test-fss3</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/provider-test-fss3</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3/_reload"
```

```
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3" rel="remove"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-test-fss3/enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">xyz,aaa,abc,cde</s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3:/b1/p1*,s3:/b2/*</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">fss3_db</s:key>
        <s:key name="disabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
<entry>
    <title> aws_s3_provider </title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/aws_s3_provider </id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">table_1,table_2</s:key>
        <s:key
name="aws_kms_keys_arn_allowlist">arn:aws:kms:us-east-1:123456789012:key/b1e51ce6-210d-49dd-a6a6-7ff950000003<
/s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3://bucket1,s3://bucket2/folder2/</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">database_1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Creates a new federated provider definition.

Request parameters

Name	What providers does this setting apply to?	Type	Description
name	All providers	String	**Required.** Specify a unique name for the federated provider.
type	All providers	String	**Required.** Set the type of federated provider. Your options for this setting depend on whether you are running your federated searches from a Splunk Enterprise deployment or Splunk Cloud Platform deployment.

Name	What providers does this setting apply to?	Type	Description
			If you are running federated searches from a Splunk Enterprise deployment, you can only set `type` to `splunk`. A setting of `type=splunk` means that you are configuring this federated provider to facilitate access to search a Splunk platform deployment. For a federated provider with `type=splunk`, you must set all settings that are required for Federated Search for Splunk providers. If you are running federated searches from a Splunk Cloud Platform deployment, you have the option of setting `type` to either `splunk` or `aws_s3`. A setting of `type=aws_s3` means that you are configuring this federated provider to facilitate access to datasets in Amazon S3. For a federated provider with `type=aws_s3`, you must set all settings that are required for Federated Search for Amazon S3 providers. Defaults to `splunk`.
mode	Applies only to Federated Search for Splunk providers	String	**Required.** Specify whether the federated provider runs federated searches in `standard` or `transparent` mode. For a detailed comparison of the standard and transparent modes of federated search, see About Federated Search for Splunk in *Federated Search*. Use transparent mode only if you are migrating to federated search from a Splunk Enterprise to Splunk Cloud Platform **hybrid search** setup. **Note:** Federated Search for Splunk does not support setting up a mix of transparent mode and standard mode federated providers for the same local deployment, as this practice can introduce unexpected complications. All of the federated providers for a specific local deployment must use the same provider mode.Defaults to `standard`.
appContext	Applies only to Federated Search for Splunk providers	String	Specify an app folder name to apply an application context to federated searches over a standard mode federated provider. The application context determines which set of knowledge objects on the remote search head is applied to the federated searches you run over that provider. • If `mode = standard`, provide the short name of an app that is installed on the remote search head of the federated provider. • If `mode = transparent`, you do not need to set `appContext`. Transparent mode federated providers ignore the `appContext` setting and instead apply the application context of the user running the federated search. See Set the app context for standard mode federated providers in *Federated Search*. Defaults to `Search`.
aws_account_id	Applies only to Federated Search for Amazon S3	Number	**Required.** Provide the 12-digit ID for the Amazon Web Services (AWS) account that is the data source for your federated provider.

Name	What providers does this setting apply to?	Type	Description
	providers		
aws_glue_tables_allowlist	Applies only to Federated Search for Amazon S3 providers	String	**Required.** Provide a comma-separated list of AWS Glue tables from which Federated Search for Amazon S3 can get metadata and data schemas. Each AWS Glue table in the list must have these elements: • It must belong to the AWS Glue Data Catalog database that you identify for the `database` setting. • It must reference an Amazon S3 location path that you have listed for the `aws_S3_paths_allowlist` setting.
aws_kms_keys_arn_allowlist	Applies only to Federated Search for Amazon S3 providers	String	If you use the AWS Key Management Service to apply server-side encryption (SSE-KMS) to the data stored in your Amazon S3 buckets, provide a comma-separated list of the Amazon resource names (ARNs) for the AWS KMS keys that encrypt Amazon S3 data. **Note:** Federated search for Amazon S3 supports only customer-managed AWS KMS keys. In addition, each KMS key ARN you provide in this field must belong to the AWS account you specify with the aws_account_id setting.
aws_s3_paths_allowlist	Applies only to Federated Search for Amazon S3 providers	String	**Required.** Provide a comma-separated list of Amazon S3 location paths that you can search with Federated Search for Amazon S3.
database	Applies only to Federated Search for Amazon S3 providers	String	**Required.** Provide the name of the AWS Glue Data Catalog database that contains the AWS Glue Data Catalog tables for the federated provider.
hostPort	Applies only to Federated Search for Splunk providers	String	**Required.** Provide the host name and port number for the federated provider, separated by a colon character. For example: `buttercupgames.splunkcloud.com:8089`.
password	Applies only to Federated Search for Splunk providers	String	**Required.** Provide the password for a service account that is already set up on the federated provider. This dedicated user account allows the federated search head on your local instance to securely search datasets on the federated provider. See Service accounts and security for Federated Search for Splunk in *Federated Search*.
serviceAccount	Applies only to Federated Search for Splunk providers	String	**Required.** Provide the username for a service account that is already set up on the federated provider. This dedicated user account allows the federated search head on your local instance to securely search datasets on the federated provider. See Service accounts and security for Federated Search for Splunk in *Federated Search*.

Returned values

Name	What providers does this setting apply to?	Description

Name	What providers does this setting apply to?	Description
name	All providers	Specifies the name of the federated provider.
type	All providers	Specifies the federated provider type. If you have a Splunk Enterprise deployment, `type` only be set to `splunk`, indicating that the provider is for Federated Search for Splunk. If you have a Splunk Cloud Platform deployment, `type` can be set either to `splunk` or `aws_s3`. A `type = aws_s3` setting indicates the provider is for Federated Search for Amazon S3. Defaults to `splunk`.
mode	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider runs federated searches in `standard` or `transparent` mode. For a detailed comparison of the standard and transparent modes of federated search, see About Federated Search for Splunk in *Federated Search*. Defaults to `standard`.
appContext	Applies only to Federated Search for Splunk providers	Specifies the Splunk application context for federated searches that are run over standard mode federated providers. The application context ensures that standard mode federated searches using this federated provider are limited to the knowledge objects that are associated with the named application. • If `mode = standard` for this federated provider, `appContext` specifies an the folder name of an app that is installed on the remote search head of the federated provider. • If `mode = transparent` for this federated provider, the federated provider ignores the `appContext` setting when you run federated searches over the provider. Transparent mode federated searches use the application context of the user running the search. Defaults to `search`.
aws_account_id	Applies only to Federated Search for Amazon S3 providers	Specifies a 12-digit Amazon Web Services (AWS) account ID.
aws_glue_tables_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of AWS Glue tables from which Federated Search for Amazon S3 can get metadata and data schemas.
aws_kms_keys_arn_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of the Amazon resource names (ARNs) for the AWS KMS keys that encrypt Amazon S3 data.
aws_region	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Web Services (AWS) region of your Splunk Cloud Platform deployment. This setting is determined automatically by Splunk software.
aws_s3_paths_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of Amazon S3 location paths that you can search with Federated Search for Amazon S3.
database	Applies only to Federated Search for Amazon S3 providers	Specifies the name of the AWS Glue Data Catalog database that contains the AWS Glue Data Catalog tables for the federated provider.
data_catalog	Applies only to Federated Search for	Specifies the Amazon Resource Name (ARN) for the AWS Glue Data Catalog. The ARN points to an AWS account. Splunk software provides the value for this setting.

Name	What providers does this setting apply to?	Description
	Amazon S3 providers	
hostPort	Applies only to Federated Search for Splunk providers	Specifies the protocols required to connect to a federated provider. Usually follows this format <Host_Name>:<Service_Port_Number>. In some cases, an IP address is used instead of a host name.
serviceAccount	Applies only to Federated Search for Splunk providers	Specifies the user name for a service account that has been set up on the federated provider for the purpose of facilitating secure federated searches.
useFSHKnowledgeObjects	Applies only to Federated Search for Splunk providers	Specifies whether the remote search head uses its own knowledge objects for federated searches, or if it uses knowledge objects that are bundle-replicated from the federated search head. The federated provider `mode` determines the required setting for `useFSHKnowledgeObjects.` • When the federated provider has `mode=standard`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `0` or `false`, which means that the federated search can use a blend of local and remote knowledge objects. • When the federated provider has `mode=transparent`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `1` or `true`, because transparent mode federated searches can use knowledge objects only from the federated search head.
connectivityStatus	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider established a connection to your local deployment in its last attempt to do so. • When `connectivityStatus=valid`, this federated provider was able to connect to your local deployment. • When `connectivityStatus=invalid`, this federated provider was unable to connect to your local deployment. • When `connectivityStatus=unknown`, the ability of the federated provider to check this connection has been turned off. This setting is for diagnostic purposes only and cannot be set or changed by users.
disabled	All providers	Specifies whether the federated provider is turned on or off. When a federated provider is turned off, the provider cannot return results for federated searches.

Example Federated Search for Splunk request and response

Create a new definition for a Federated Search for Splunk federated provider named `provider-1`.

XML request

```
curl -k -u admin:changeme -X POST https://localhost:8126/services/data/federated/provider -d
name=provider-1 -d type=splunk -d mode=standard -d hostPort=10.225.131.242:8089 -d serviceAccount=admin -d
password=Chang3d!
```

XML response

```
...
  <entry>
```

```
    <title>provider-1</title>
    <id>https://localhost:8126/servicesNS/nobody/system/data/federated/provider/provider-1</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-1" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-1" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-1/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-1" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/provider-1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="appContext">search</s:key>
        <s:key name="connectivityStatus">unknown</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="hostPort">10.225.131.242:8089</s:key>
        <s:key name="mode">standard</s:key>
        <s:key name="serviceAccount">admin</s:key>
        <s:key name="type">splunk</s:key>
        <s:key name="useFSHKnowledgeObjects">0</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

Example Federated Search for Amazon S3 request and response

Create a new definition for a Federated Search for Splunk federated provider named `aws_s3_provider`.

XML request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/data/federated/provider -d
name=aws_s3_provider -d type=aws_s3 -d aws_account_id=123456789012 -d database=database_1 -d
aws_s3_paths_allowlist="s3://bucket1,s3://bucket2/folder2/" -d
aws_kms_keys_arn_allowlist=arn:aws:kms:us-east-1:123456789012:key/b1e51ce6-210d-49dd-a6a6-7ff950000003 -d
aws_glue_tables_allowlist=table_1,table_2
```

XML response

```
...
<entry>
    <title>test_provider</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/aws_s3_provider</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">table_1,table_2</s:key>
        <s:key
name="aws_kms_keys_arn_allowlist">arn:aws:kms:us-east-1:123456789012:key/b1e51ce6-210d-49dd-a6a6-7ff950000003<
/s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3://bucket1,s3://bucket2/folder2/</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">database_1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/federated/provider/turnOffProvidersInBatch

`https://<host>:<mPort>/services/data/federated/provider/turnOffProvidersInBatch`

Use this endpoint to turn off groups of federated providers with one REST API call. This endpoint applies to federated providers for Federated Search for Splunk and Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform.

When federated providers are turned off, their federated indexes are unavailable for federated searches.

After you turn off a group of federated providers with this endpoint, individually turn each deactivated federated provider back on with the data/federated/provider/{federated_provider_name}/enable endpoint.

> The provider endpoint does not honor user or app context. It always places federated provider stanzas in etc/system/local/federated.conf, no matter which user or app namespace you are currently using.

For more information about defining federated providers for Federated Search for Splunk, see Define a Splunk platform federated provider in *Federated Search*.

For more information about defining federated providers for Federated Search for Amazon S3, see Define an Amazon S3 federated provider in *Federated Search*.

Authentication and authorization

Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects **capability**.

POST

Turns off all federated providers. Can also turn off all federated providers belonging to a specific federated search `type`.

Request parameters

Name	What providers does this setting apply to?	Type	Description
type	All providers	String	**Optional** Provide a filter for the federated provider type. Your options for this setting depend on whether you are using Splunk Enterprise or Splunk Cloud Platform. If you are running federated searches from a Splunk Enterprise deployment, you can only filter on `type=splunk`. A filter of `type=splunk` turns off all federated providers for Federated Search for Splunk. If you are running federated searches from a Splunk Cloud Platform deployment, you have the option of filtering on `type=splunk` or `type=aws_s3`. A filter of `type=aws_s3` turns off all federated providers for Federated Search for Amazon

Name	What providers does this setting apply to?	Type	Description
			S3. No default.

Returned values

None specific to this method.

Example XML requests

Turn off all federated providers, regardless of `type`.

```
curl -k -u admin:changeme -X POST
https://localhost:8089/services/data/federated/provider/turnOffProvidersInBatch
```

Turn off all Federated Search for Splunk federated providers.

```
curl -k -u admin:changeme --request -X POST
https://localhost:8089/services/data/federated/provider/turnOffProvidersInBatch -d type=splunk
```

Turn off all Federated Search for Amazon S3 federated providers.

```
curl -k -u admin:changeme --request -X POST
https://localhost:8089/services/data/federated/provider/turnOffProvidersInBatch -d  type=aws_s3
```

XML response

```
  <title>federated-provider</title>
  <id>https://localhost:8089/services/data/federated/provider</id>
  <updated>2024-01-12T15:42:21-08:00</updated>
  <generator build="560faafdef34420e5bda25009961db864cef5986" version="20240110"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/provider/_new" rel="create"/>
  <link href="/services/data/federated/provider/_reload" rel="_reload"/>
  <link href="/services/data/federated/provider/_acl" rel="_acl"/>
  <link href="/services/data/federated/provider/generateACSPolicy" rel="generateACSPolicy"/>
  <link href="/services/data/federated/provider/generatePolicy" rel="generatePolicy"/>
  <link href="/services/data/federated/provider/getACSPolicy" rel="getACSPolicy"/>
  <link href="/services/data/federated/provider/getRegion" rel="getRegion"/>
  <link href="/services/data/federated/provider/turnOffProvidersInBatch" rel="turnOffProvidersInBatch"/>
  <link href="/services/data/federated/provider/updateACSPolicy" rel="updateACSPolicy"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/federated/provider/{federated_provider_name}

`https://<host>:<mPort>/services/data/federated/provider/{federated_provider_name}`

Use this endpoint to:

- Retrieve a specific federated provider definition.
- Update a specific federated provider definition.
- Delete a specific federated provider definition.

Some of the settings you can review and update with these endpoints are exclusive to Federated Search for Splunk, while other settings are exclusive to Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform deployments.

> The provider endpoint does not honor user or app context. It always places federated provider stanzas in etc/system/local/federated.conf, no matter which user or app namespace you are currently using.

For more information about defining federated providers for Federated Search for Splunk, see Define a Splunk platform federated provider in *Federated Search*.

For more information about defining federated providers for Federated Search for Amazon S3, see Define an Amazon S3 federated provider in *Federated Search*.

Authentication and Authorization

Usage of the POST and DELETE operations for this endpoint is restricted to roles that have the admin_all_objects **capability**.

GET

Returns a definition of a specific `{federated_provider_name}`.

Request parameters

None specific to this method.

Returned values

Name	What providers does this setting apply to?	Description
name	All providers	Specifies the name of the federated provider.
type	All providers	Specifies the federated provider type. If you have a Splunk Enterprise deployment, you can set `type` only to `splunk`, indicating that the provider is for Federated Search for Splunk. If you have a Splunk Cloud Platform deployment, you can set `type` to either `splunk` or `aws_s3`. A `type = aws_s3` setting indicates the provider is for Federated Search for Amazon S3. Defaults to `splunk`.
mode	Applies only to Federated Search for	Specifies whether the federated provider runs federated searches in `standard` or `transparent` mode. For a detailed comparison of the standard and transparent modes

Name	What providers does this setting apply to?	Description
	Splunk providers	of federated search, see About Federated Search for Splunk in *Federated Search*. Defaults to `standard`.
appContext	Applies only to Federated Search for Splunk providers	Specifies the Splunk application context for federated searches that are run over standard mode federated providers. The application context ensures that standard mode federated searches using this federated provider are limited to the knowledge objects that are associated with the named application. • If `mode = standard` for this federated provider, `appContext` specifies an the folder name of an app that is installed on the remote search head of the federated provider. • If `mode = transparent` for this federated provider, the federated provider ignores the `appContext` setting when you run federated searches over the provider. Transparent mode federated searches use the application context of the user running the search. Defaults to `search`.
aws_account_id	Applies only to Federated Search for Amazon S3 providers	Specifies a 12-digit Amazon Web Services (AWS) account ID.
aws_glue_tables_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of AWS Glue tables from which Federated Search for Amazon S3 can get metadata and data schemas.
aws_kms_keys_arn_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of the Amazon resource names (ARNs) for the AWS KMS keys that encrypt Amazon S3 data.
aws_region	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Web Services (AWS) region of your Splunk Cloud Platform deployment. This setting is determined automatically by Splunk software.
aws_s3_paths_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of Amazon S3 location paths that you can search with Federated Search for Amazon S3.
database	Applies only to Federated Search for Amazon S3 providers	Specifies the name of the AWS Glue Data Catalog database that contains the AWS Glue Data Catalog tables for the federated provider.
data_catalog	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Resource Name (ARN) for the AWS Glue Data Catalog. The ARN points to an AWS account.
hostPort	Applies only to Federated Search for Splunk providers	Specifies the protocols required to connect to a federated provider. Usually follows this format <Host_Name>:<Service_Port_Number>. In some cases, an IP address is used instead of a host name.
serviceAccount	Applies only to Federated Search for Splunk providers	Specifies the user name for a service account that has been set up on the federated provider for the purpose of facilitating secure federated searches.
useFSHKnowledgeObjects	Applies only to Federated Search for Splunk providers	Specifies whether the remote search head uses its own knowledge objects for federated searches, or if it uses knowledge objects that are bundle-replicated from the federated search head.

Name	What providers does this setting apply to?	Description
		The federated provider `mode` determines the required setting for `useFSHKnowledgeObjects.` • When the federated provider has `mode=standard`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `0` or `false`, which means that the federated search can use a blend of local and remote knowledge objects. • When the federated provider has `mode=transparent`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `1` or `true`, because transparent mode federated searches can use knowledge objects only from the federated search head.
connectivityStatus	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider established a connection to your local deployment in its last attempt to do so. • When `connectivityStatus=valid`, this federated provider was able to connect to your local deployment. • When `connectivityStatus=invalid`, this federated provider was unable to connect to your local deployment. • When `connectivityStatus=unknown`, the ability of the federated provider to check this connection has been turned off. This setting is for diagnostic purposes only and cannot be set or changed by users.
disabled	All providers	Specifies whether the federated provider is turned on or off. When a federated provider is turned off, the provider cannot return results for federated searches.

Example Federated Search for Splunk request and response

Return the definition for the `my_federated_provider` federated provider.

XML Request

```
curl -k -u admin:changeme -X GET
 https://localhost:8089/services/data/federated/provider/my_federated_provider
```

XML response

```
...
<entry>
  <title>my_federated_provider</title>
  <id>/servicesNS/nobody/system/data/federated/provider/my_federated_provider</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="list"/>
  <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider/_reload"
rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="remove"/>
  <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider/disable"
```

```
rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="appContext">search</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>appContext</s:item>
              <s:item>hostPort</s:item>
              <s:item>password</s:item>
              <s:item>serviceAccount</s:item>
              <s:item>type</s:item>
              <s:item>useFSHKnowledgeObjects</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list>
              <s:item>.*</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="hostPort">10.225.131.242:8089</s:key>
      <s:key name="mode">standard</s:key>
      <s:key name="serviceAccount">user1</s:key>
      <s:key name="type">splunk</s:key>
      <s:key name="useFSHKnowledgeObjects">1</s:key>
    </s:dict>
  </content>
</entry>
```

Example Federated Search for Amazon S3 request and response

Return the definition for the `aws_s3_provider` federated provider.

XML Request

```
curl -k -u admin:changeme -X GET https://localhost:8089/services/data/federated/provider/aws_s3_provider
```

XML response

```
...
  <entry>
    <title> aws_s3_provider</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/aws_s3_provider</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">table_1,table_2</s:key>
        <s:key
name="aws_kms_keys_arn_allowlist">arn:aws:kms:us-east-1:123456789012:key/b1e51ce6-210d-49dd-a6a6-7ff950000003<
/s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3://bucket1,s3://bucket2/folder2/</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">database_1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Updates a definition for a specific `{federated_provider_name}`.

Request parameters

At least one argument is required.

Name	What providers does this setting apply to?	Type	Description
appContext	Applies only to Federated Search for Splunk providers	String	Specify an app folder name to apply an application context to federated searches over a standard mode federated provider. The application context determines which set of knowledge objects on the remote search head is applied to the federated searches you run over that provider. - If `mode = standard`, provide the short name of an app that is installed on the remote search head of the federated provider. - If `mode = transparent`, you do not need to set `appContext`. Transparent mode federated providers ignore the `appContext` setting and instead apply the application context of the user running the federated search. See Set the app context for standard mode federated providers in *Federated Search*. Defaults to `Search`.
aws_account_id	Applies only to Federated Search for Amazon S3 providers	Number	**Required.** Provide the 12-digit ID for the Amazon Web Services (AWS) account that is the data source for your federated provider.
aws_glue_tables_allowlist	Applies only to Federated Search for Amazon S3 providers	String	**Required.** Provide a comma-separated list of AWS Glue tables from which Federated Search for Amazon S3 can get metadata and data schemas. Each AWS Glue table in the list must have these elements: - It must belong to the AWS Glue Data Catalog database that you identify for the `database` setting. - It must reference an Amazon S3 location path that you have listed for the `aws_S3_paths_allowlist` setting.
aws_kms_keys_arn_allowlist	Applies only to Federated Search for Amazon S3 providers	String	If you use the AWS Key Management Service to apply server-side encryption (SSE-KMS) to the data stored in your Amazon S3 buckets, provide a comma-separated list of the Amazon resource names (ARNs) for the AWS KMS keys that encrypt Amazon S3 data. **Note:** Federated search for Amazon S3 supports only customer-managed AWS KMS keys. In addition, each KMS key ARN

Name	What providers does this setting apply to?	Type	Description
			you provide in this field must belong to the AWS account you specify with the aws_account_id setting.
aws_s3_paths_allowlist	Applies only to Federated Search for Amazon S3 providers	String	**Required.** Provide a comma-separated list of Amazon S3 location paths that you can search with Federated Search for Amazon S3.
hostPort	Applies only to Federated Search for Splunk providers	String	**Required.** Provide the host name and port number for the federated provider, separated by a colon character. For example: `buttercupgames.splunkcloud.com:8089`.
password	Applies only to Federated Search for Splunk providers	String	**Required.** Provide the password for a service account that is already set up on the federated provider. This dedicated user account allows the federated search head on your local instance to securely search datasets on the federated provider. See Service accounts and security for Federated Search for Splunk in *Federated Search*.
serviceAccount	Applies only to Federated Search for Splunk providers	String	**Required.** Provide the username for a service account that is already set up on the federated provider. This dedicated user account allows the federated search head on your local instance to securely search datasets on the federated provider. See Service accounts and security for Federated Search for Splunk in *Federated Search*.

Returned values

Name	What providers does this setting apply to?	Description
name	All providers	Specifies the name of the federated provider.
type	All providers	Specifies the federated provider type. If you have a Splunk Enterprise deployment, you can set `type` only to `splunk`, indicating that the provider is for Federated Search for Splunk. If you have a Splunk Cloud Platform deployment, you can set `type` to either `splunk` or `aws_s3`. A `type = aws_s3` setting indicates the provider is for Federated Search for Amazon S3. Defaults to `splunk`.
mode	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider runs federated searches in `standard` or `transparent` mode. For a detailed comparison of the standard and transparent modes of federated search, see About Federated Search for Splunk in *Federated Search*. Defaults to `standard`.
appContext	Applies only to Federated Search for Splunk providers	Specifies the Splunk application context for federated searches that are run over standard mode federated providers. The application context ensures that standard mode federated searches using this federated provider are limited to the knowledge objects

Name	What providers does this setting apply to?	Description
		that are associated with the named application. - If `mode = standard` for this federated provider, `appContext` specifies an the folder name of an app that is installed on the remote search head of the federated provider. - If `mode = transparent` for this federated provider, the federated provider ignores the `appContext` setting when you run federated searches over the provider. Transparent mode federated searches use the application context of the user running the search. Defaults to `search`.
aws_account_id	Applies only to Federated Search for Amazon S3 providers	Specifies a 12-digit Amazon Web Services (AWS) account ID.
aws_glue_tables_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of AWS Glue tables from which Federated Search for Amazon S3 can get metadata and data schemas.
aws_kms_keys_arn_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of the Amazon resource names (ARNs) for the AWS KMS keys that encrypt Amazon S3 data.
aws_region	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Web Services (AWS) region of your Splunk Cloud Platform deployment. This setting is determined automatically by Splunk software.
aws_s3_paths_allowlist	Applies only to Federated Search for Amazon S3 providers	Specifies a comma-separated list of Amazon S3 location paths that you can search with Federated Search for Amazon S3.
database	Applies only to Federated Search for Amazon S3 providers	Specifies the name of the AWS Glue Data Catalog database that contains the AWS Glue Data Catalog tables for the federated provider.
data_catalog	Applies only to Federated Search for Amazon S3 providers	Specifies the Amazon Resource Name (ARN) for the AWS Glue Data Catalog. The ARN points to an AWS account. Splunk software provides the value for this setting.
hostPort	Applies only to Federated Search for Splunk providers	Specifies the protocols required to connect to a federated provider. Usually follows this format <Host_Name>:<Service_Port_Number>. In some cases, an IP address is used instead of a host name.
serviceAccount	Applies only to Federated Search for Splunk providers	Specifies the user name for a service account that has been set up on the federated provider for the purpose of facilitating secure federated searches.
useFSHKnowledgeObjects	Applies only to Federated Search for Splunk providers	Specifies whether the remote search head uses its own knowledge objects for federated searches, or if it uses knowledge objects that are bundle-replicated from the federated search head. The federated provider `mode` determines the required setting for `useFSHKnowledgeObjects`. - When the federated provider has `mode=standard`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `0` or `false`, which means that the federated search can use a blend of local and remote

Name	What providers does this setting apply to?	Description
		knowledge objects. - When the federated provider has `mode=transparent`, Splunk software always interprets `useFSHKnowledgeObjects` as being set to `1` or `true`, because transparent mode federated searches can use knowledge objects only from the federated search head.
connectivityStatus	Applies only to Federated Search for Splunk providers	Specifies whether the federated provider established a connection to your local deployment in its last attempt to do so. - When `connectivityStatus=valid`, this federated provider was able to connect to your local deployment. - When `connectivityStatus=invalid`, this federated provider was unable to connect to your local deployment. - When `connectivityStatus=unknown`, the ability of the federated provider to check this connection has been turned off. This setting is for diagnostic purposes only and cannot be set or changed by users.
disabled	All providers	Specifies whether the federated provider is turned on or off. When a federated provider is turned off, the provider cannot return results for federated searches.

Example Federated Search for Splunk request and response

For the federated provider named `my_federated_provider`, change the `serviceAccount` setting to `eagle01`, to match an update to the service account user on that federated provider.

XML request

```
curl -k -u admin:changeme -X POST
https://localhost:8089/services/data/federated/provider/my_federated_provider -d serviceAccount=eagle01
```

XML response

```
  <entry>
    <title>my_federated_provider</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/my_federated_provider</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/my_federated_provider" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="appContext">search</s:key>
       <s:key name="connectivityStatus">valid</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="hostPort">10.224.150.77:58677</s:key>
        <s:key name="mode">standard</s:key>
        <s:key name="serviceAccount">eagle01</s:key>
        <s:key name="type">splunk</s:key>
        <s:key name="useFSHKnowledgeObjects">0</s:key>
      </s:dict>
    </content>
  </entry>
```

Example Federated Search for Amazon S3 request and response

For the federated provider named `aws_s3_provider` , change the `aws_glue_tables_allowlist` setting to `table_1,table_2,table3,table4`, to include `table3` and `table4`, two new AWS Glue tables that you added to the AWS Glue database.

XML request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/data/federated/provider/aws_s3_provider -d
aws_glue_tables_allowlist=table_1,table_2,table3,table4
```

XML response

```
  <entry>
    <title>test_provider</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/federated/provider/aws_s3_provider</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="list"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/federated/provider/aws_s3_provider" rel="remove"/>
    <content type="text/xml">
```

```
      <s:dict>
        <s:key name="aws_account_id">123456789012</s:key>
        <s:key name="aws_glue_tables_allowlist">table3,table4,table_1,table_2</s:key>
        <s:key
name="aws_kms_keys_arn_allowlist">arn:aws:kms:us-east-1:123456789012:key/b1e51ce6-210d-49dd-a6a6-7ff950000003<
/s:key>
        <s:key name="aws_region">us-west-2</s:key>
        <s:key name="aws_s3_paths_allowlist">s3://bucket1,s3://bucket2/folder2/</s:key>
        <s:key name="data_catalog">glue:arn:aws:glue:us-west-2:123456789012:catalog</s:key>
        <s:key name="database">database_1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="type">aws_s3</s:key>
      </s:dict>
    </content>
  </entry>
```

DELETE

Deletes a definition for a specific `{federated_provider_name}`.

Request parameters

None specific to this method.

Returned values

None specific to this method.

Example Federated Search for Splunk request and response

Delete the `[provider://my_federated_provider]` stanza from etc/system/local/federated.conf.

XML Request

```
curl -k -u admin:changeme -X DELETE
https://localhost:8089/services/data/federated/provider/my_federated_provider
```

XML response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>federated-provider</title>
  <id>/services/data/federated/provider</id>
  <updated>2021-04-27T12:47:36-07:00</updated>
  <generator build="aa7e77c0d232b8ec1a8c12ceeda95e0bfe3c3f1c" version="20210423"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/provider/_new" rel="create"/>
  <link href="/services/data/federated/provider/_reload" rel="_reload"/>
  <link href="/services/data/federated/provider/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

Example Federated Search for Amazon S3 request and response

Delete the `[provider://aws_s3_provider]` stanza from etc/system/local/federated.conf.

XML Request

```
curl -k -u admin:changeme -X DELETE https://localhost:8089/services/data/federated/provider/aws_s3_provider
```

XML Response

```
  <title>federated-provider</title>
  <id>https://localhost:8089/services/data/federated/provider</id>
  <updated>2024-01-12T16:15:18-08:00</updated>
  <generator build="560faafdef34420e5bda25009961db864cef5986" version="20240110"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/provider/_new" rel="create"/>
  <link href="/services/data/federated/provider/_reload" rel="_reload"/>
  <link href="/services/data/federated/provider/_acl" rel="_acl"/>
  <link href="/services/data/federated/provider/generateACSPolicy" rel="generateACSPolicy"/>
  <link href="/services/data/federated/provider/generatePolicy" rel="generatePolicy"/>
  <link href="/services/data/federated/provider/getACSPolicy" rel="getACSPolicy"/>
  <link href="/services/data/federated/provider/getRegion" rel="getRegion"/>
  <link href="/services/data/federated/provider/turnOffProvidersInBatch" rel="turnOffProvidersInBatch"/>
  <link href="/services/data/federated/provider/updateACSPolicy" rel="updateACSPolicy"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/federated/provider/{federated_provider_name}/disable

`https://<host>:<mPort>/services/data/federated/provider/{federated_provider_name}/disable`

Use this endpoint to turn a specific federated provider off. When a federated provider is turned off, all federated indexes associated with that provider are not searchable in federated searches. This endpoint applies to federated providers for Federated Search for Splunk and for Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform deployments.

> The provider endpoint does not honor user or app context. It always places federated provider stanzas in etc/system/local/federated.conf, no matter which user or app namespace you are currently using.

For more information about federated providers for Federated Search for Splunk, see Define a Splunk platform federated provider in *Federated Search*.

For more information about federated providers for Federated Search for Amazon S3, see Define an Amazon S3 federated provider in *Federated Search*.

Authentication and Authorization
Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects **capability**.

POST

Turn off a specific federated provider.

Request parameters
None specific to this method.

Returned values
None specific to this method.

Example federated search request and response
Turn off a provider named `aws_s3_provider`.

XML request

```
curl -k -u admin:changeme --request -X POST
https://localhost:8089/services/data/federated/provider/aws_s3_provider/disable
```

XML response

```
  <entry>
    <title>federated-provider</title>
  <id>https://localhost:8089/services/data/federated/provider</id>
  <updated>2024-01-12T15:42:21-08:00</updated>
  <generator build="560faafdef34420e5bda25009961db864cef5986" version="20240110"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/provider/_new" rel="create"/>
  <link href="/services/data/federated/provider/_reload" rel="_reload"/>
  <link href="/services/data/federated/provider/_acl" rel="_acl"/>
  <link href="/services/data/federated/provider/generateACSPolicy" rel="generateACSPolicy"/>
  <link href="/services/data/federated/provider/generatePolicy" rel="generatePolicy"/>
  <link href="/services/data/federated/provider/getACSPolicy" rel="getACSPolicy"/>
  <link href="/services/data/federated/provider/getRegion" rel="getRegion"/>
  <link href="/services/data/federated/provider/turnOffProvidersInBatch" rel="turnOffProvidersInBatch"/>
  <link href="/services/data/federated/provider/updateACSPolicy" rel="updateACSPolicy"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/federated/provider/{federated_provider_name}/enable

`https://<host>:<mPort>/services/data/federated/provider/{federated_provider_name}/enable`

Use this endpoint to turn a federated provider back on after you have turned it off. When a federated provider is turned on, all federated indexes associated with that provider can be searched in federated searches. This endpoint applies to federated providers for Federated Search for Splunk and federated providers for Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform deployments.

> The provider endpoint does not honor user or app context. It always places federated provider stanzas in etc/system/local/federated.conf, no matter which user or app namespace you are currently using.

For more information about federated providers for Federated Search for Splunk, see Define a Splunk platform federated provider in *Federated Search*.

For more information about federated providers for Federated Search for Amazon S3, see Define an Amazon S3 federated provider in *Federated Search*.

Authentication and Authorization

Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects **capability**.

POST

Turns a specific federated index on.

Request parameters

None specific to this method.

Returned values

None specific to this method.

Example request and response

Turn on a federated provider named `aws_s3_provider`.

XML request

```
curl -k -u admin:changeme --request -X POST
 https://localhost:8089/services/data/federated/provider/aws_s3_provider/enable
```

XML response

```
  <title>federated-provider</title>
  <id>https://localhost:8089/services/data/federated/provider</id>
  <updated>2024-01-12T15:42:21-08:00</updated>
  <generator build="560faafdef34420e5bda25009961db864cef5986" version="20240110"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/provider/_new" rel="create"/>
  <link href="/services/data/federated/provider/_reload" rel="_reload"/>
  <link href="/services/data/federated/provider/_acl" rel="_acl"/>
  <link href="/services/data/federated/provider/generateACSPolicy" rel="generateACSPolicy"/>
  <link href="/services/data/federated/provider/generatePolicy" rel="generatePolicy"/>
  <link href="/services/data/federated/provider/getACSPolicy" rel="getACSPolicy"/>
  <link href="/services/data/federated/provider/getRegion" rel="getRegion"/>
  <link href="/services/data/federated/provider/turnOffProvidersInBatch" rel="turnOffProvidersInBatch"/>
  <link href="/services/data/federated/provider/updateACSPolicy" rel="updateACSPolicy"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/federated/index

`https://<host>:<mPort>/services/data/federated/index`

Use this endpoint to get a list of federated indexes and post new federated index definitions. Some of these federated index settings are exclusive to Federated Search for Splunk, while others are exclusive to Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform.

For more information about defining federated indexes for Federated Search for Splunk, see Map a federated index to a remote Splunk dataset in *Federated Search.*

For more information about defining federated indexes for Federated Search for Amazon S3, see Map a federated index to an AWS Glue Data Catalog table dataset in *Federated Search*.

Authentication and authorization

Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects and indexes_edit **capabilities**.

GET

Returns a list of federated indexes.

Request parameters

None specific to this method. This method can use pagination and filtering parameters.

Returned values

This table is limited to settings specific to federated indexes. For descriptions of other index settings see the entry for `data/indexes`.

> The data/indexes endpoint is available only to users of Splunk Enterprise.

Name	What kinds of federated indexes does this setting apply to?	Description
name	All federated indexes	Specifies the name of the federated index. Uses the syntax `federated:<index_name>`.
federated.provider	All federated indexes	Specifies the federated provider that contains the dataset to which this federated index maps.
federated.dataset	All federated indexes	Specifies the remote dataset on the `federated.provider` to which this federated index maps. Each federated index maps to only one dataset on a federated provider. The dataset is identified by its prefix and name, using the following syntax: `<prefix>:<dataset_name>`. If the `federated.provider` has `type=splunk` in its definition on federated.conf, the possible values for `<prefix>` are `index`, `metricindex`, `savedsearch`, `lastjob`, and `datamodel`. If the `federated.provider` has `type=aws_s3` in its definition on federated.conf, the `<prefix>` must be set to `aws_glue_table`.
federated.timefield	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time field that acts like an event timestamp in the AWS Glue table to which this index maps.
federated.timeformat	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time format variable or custom time format variable string that matches the `federated.timefield`.
federated.unixtimefield	Applies only to Federated Search for Amazon S3 federated indexes	An alias for the `federated.timefield` that Splunk software converts into numeric UNIX time format at search time. Insert the `federated.unixtimefield` into federated searches that require numeric UNIX time field values, or when you want to see your time field in numeric UNIX time format in the search results. Defaults to `_time`.
federated.partition.time.fields	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time-related fields in the AWS Glue table to which the index is mapped. Each field is a partition key for a partition time field level indicated by its order in the list. The first field is at the first level, the second field is at the second level, and so on.
federated.partition.time.formats	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time format variables or custom time format strings that correspond to the fields in the `federated.partition.time.fields` list. The first variable corresponds to the first field name, the second variable corresponds to the second field name, and so on.
federated.partition.time.types	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time field types that correspond to the fields in the `federated.partition.time.fields` list. Possible values are `String`, `Integer`, and `Date`.
federated.partition.time.tz	Applies only to Federated Search for	Specifies the timezone that corresponds to the fields in the `federated.partition.time.fields` list. Possible values are canonical

Name	What kinds of federated indexes does this setting apply to?	Description
	Amazon S3 federated indexes	timezone names such as `America/Los_Angeles`.

Example request and response

Get the complete list of federated indexes. The following XML response provides a sample of one returned Federated Search for Splunk federated index record.

XML Request

```
curl -k -u admin:changeme -X GET  https://localhost:8126/services/data/federated/index
```

XML response

```
...
  <entry>
    <title>federated:remote_index_df_1</title>
    <id>https://localhost:8126/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1<
/id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">index:index_df_1</s:key>
        <s:key name="federated.provider">provider-1</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Creates a new federated index definition.

These tables are limited to settings specific to federated indexes. For descriptions of other index settings see the entry for `data/indexes`.

The data/indexes endpoint is available only to users of Splunk Enterprise.

Request parameters

Name	What kinds of federated indexes does this setting apply to?	Type	Description
name	All federated indexes	String	**Required.** Specify a unique name for the federated index, using the syntax `federated:<index_name>`. Each federated index maps to only one remote dataset on a federated provider, so the name should reference that dataset. Index names have the following limitations: • They may contain only lowercase letters, numbers, underscores, and hyphens. • They must begin with a letter or number. • They cannot be more than 2048 characters in length. • They cannot contain the string "kvstore".
federated.provider	All federated indexes	String	**Required.** Specify the federated provider that contains the dataset to which this federated index maps.
federated.dataset	All federated indexes	String	**Required.** Specify the dataset on the `federated.provider` to which this federated index maps. The dataset is identified by its type and name, using the following syntax: `<prefix>:<remote_name>`. If the `federated.provider` has `type=splunk` in its definition on `federated.conf`, the possible values for `<prefix>` are: • `index`: A name of an events index on the federated provider. Each remote events index is a searchable dataset.

Name	What kinds of federated indexes does this setting apply to?	Type	Description
			- `metricindex`: A name of a metrics index on the federated provider. Each remote metrics index is a searchable dataset. - `savedsearch`: A name of a saved search on the federated provider. The result set produced by an ad-hoc run of a saved search is a searchable dataset. - `lastjob`: A name of a saved search on the federated provider that has been configured to run on a schedule. The result set for the last job run for a scheduled search is a searchable dataset. - `datamodel`: A name of a **data model** on the federated provider. The set of events defined by a data model is a searchable dataset. If the `federated.provider` has `type=aws_s3` in its definition on `federated.conf`, the `<prefix>` must be set to `aws_glue_table`, and the `<remote_name>` must be set to the name of an AWS Glue Data Catalog table that is listed in the `federated.provider` definition in `federated.conf`. An AWS Glue Data Catalog table contains metadata that represents data in an Amazon S3 data store. If the `<prefix>` is undefined, it defaults to `index`. There is no default value for the `<remote_name>`.
federated.timefield	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies the name of a time field that acts like an event timestamp in the AWS Glue table to which this index maps. In other words, the name of the field in the AWS Glue table that behaves like `_time` in the Splunk search processing language. You must provide a `federated.timefield` if you want to use time-related functions to search your remote Amazon S3 data.
federated.timeformat	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies the time format variable or custom time format variable string that matches the `federated.timefield`. The time format variable string must be in Splunk `strptime()` format. This setting is required if you provide a `federated.timefield` value.
federated.unixtimefield	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies an alias for the `federated.timefield` that Splunk software converts into numeric UNIX time format at search time. Insert the `federated.unixtimefield` into federated searches that require numeric UNIX time field values, or when you want to see your time field in numeric UNIX time format in the search results. The `federated.timefield` for a federated index cannot have the same value as the `federated.unixtimefield` for that federated index. In other words, if `federated.timefield` is set to `_time`, you must change the value of `federated.unixtimefield` to a value other than `_time`. Defaults to `_time`.

Name	What kinds of federated indexes does this setting apply to?	Type	Description
federated.partition.time.fields	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies a comma-delimited list of time-related fields in your remote data. These fields govern the partitions by which remote data is organized in non-Splunk-platform federated providers (such as Amazon S3 federated providers). Use this setting in conjunction with `federated.partition.time.formats` and `federated.partition.time.types` to identify the hierarchical structure of the data partitions in your remote data. The field list you provide for `federated.partition.time.fields` must correspond with the list of time formats you provide for `federated.partition.time.formats` and the list of data types you provide for `federated.partition.time.types`. Time field names containing comma characters must be surrounded by double quote characters to prevent Splunk software from breaking such values into multiple values. Do not set `federated.partition.time.fields` if the federated provider with which the federated index is associated has `type=splunk`.
federated.partition.time.formats	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies a comma-delimited list of time format variable strings that correspond to the time fields listed by the `federated.partition.time.fields` setting. The '%w'; and '%JT' time format variables are not supported by this setting. See Date and time format variables in the *Search manual*. Time format variable strings containing comma characters must be surrounded by double-quote characters to prevent Splunk software from breaking such strings into multiple values. This setting is required if you have defined a list of `federated.partition.time.fields`. Do not set this setting if `federated.partition.time.fields` is not set.
federated.partition.time.types	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies a comma-delimited list of data type values that correspond to the time fields listed by the `federated.partition.time.fields` setting. The supported time field types are `string`, `integer`, and `date`. This setting is required if you have defined a list of `federated.partition.time.fields`. Do not set this setting if `federated.partition.time.fields` is not set.
federated.partition.time.tz		String	

Name	What kinds of federated indexes does this setting apply to?	Type	Description
	Applies only to Federated Search for Amazon S3 federated indexes		**Optional.** Specifies the time zone to use for the time fields listed in `federated.partition.time.fields`. Use only canonical time zone names such as `America/Los_Angeles`. Do not set this setting if `federated.partition.time.fields` is not set. If this setting is not set when `federated.partition.time.fields` is set, Splunk software uses the per-user time zone, as declared in user-prefs.conf with the `tz` setting.

Returned values

This table is limited to settings specific to federated indexes. For descriptions of other index settings see the entry for `data/indexes`.

> The data/indexes endpoint is available only to users of Splunk Enterprise.

Name	What kinds of federated indexes does this setting apply to?	Description
name	All federated indexes	Specifies the name of the federated index. Uses the syntax `federated:<index_name>`.
federated.provider	All federated indexes	Specifies the federated provider that contains the dataset to which this federated index maps.
federated.dataset	All federated indexes	Specifies the remote dataset on the `federated.provider` to which this federated index maps. Each federated index maps to only one dataset on a federated provider. The dataset is identified by its prefix and name, using the following syntax: `<prefix>:<dataset_name>`. If the `federated.provider` has `type=splunk` in its definition on federated.conf, the possible values for `<prefix>` are `index`, `metricindex`, `savedsearch`, `lastjob`, and `datamodel`. If the `federated.provider` has `type=aws_s3` in its definition on federated.conf, the `<prefix>` must be set to `aws_glue_table`.
federated.timefield	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time field in the AWS Glue table to which this index maps that acts like an event timestamp.
federated.timeformat	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time format variable or custom time format variable string that matches the `federated.timefield`.

Name	What kinds of federated indexes does this setting apply to?	Description
federated.unixtimefield	Applies only to Federated Search for Amazon S3 federated indexes	An alias for the `federated.timefield` that Splunk software converts into numeric UNIX time format at search time. Insert the `federated.unixtimefield` into federated searches that require numeric UNIX time field values, or when you want to see your time field in numeric UNIX time format in the search results. Defaults to `_time`.
federated.partition.time.fields	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time-related fields in the AWS Glue table to which the index is mapped. Each field is a partition key for a partition time field level indicated by its order in the list. The first field is at the first level, the second field is at the second level, and so on.
federated.partition.time.formats	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time format variables or custom time format strings that correspond to the fields in the `federated.partition.time.fields` list. The first variable corresponds to the first field name, the second variable corresponds to the second field name, and so on.
federated.partition.time.types	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time field types that correspond to the fields in the `federated.partition.time.fields` list. Possible values are `String`, `Integer`, and `Date`.
federated.partition.time.tz	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the timezone that corresponds to the fields in the `federated.partition.time.fields` list. Possible values are canonical timezone names such as `America/Los_Angeles`.

Example Federated Search for Splunk request and response

Create a new definition for a Federated Search for Splunk federated index named `airports-east`.

XML Request

```
curl -k -u admin:changeme -X POST  https://localhost:8089/services/data/federated/index -d
name=federated:airports-east -d federated.provider=FenrisAirNYC -d federated.dataset=index:airports-east
```

XML response

```
<entry>
  <title>federated:fs-airports-east</title>
  <id>/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east" rel="list"/>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east/_reload"
rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east" rel="edit"/>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east" rel="remove"/>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east/move" rel="move"/>
  <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east/disable"
```

```
rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="assureUTF8">0</s:key>
      <s:key name="bucketMerge.maxMergeSizeMB">1000</s:key>
      <s:key name="bucketMerge.maxMergeTimeSpanSecs">7776000</s:key>
      <s:key name="bucketMerge.minMergeSizeMB">750</s:key>
      <s:key name="bucketMerging">0</s:key>
      <s:key name="coldPath.maxDataSizeMB">0</s:key>
      <s:key name="coldToFrozenDir"></s:key>
      <s:key name="coldToFrozenScript"></s:key>
      <s:key name="compressRawdata">1</s:key>
      <s:key name="datatype">event</s:key>
      <s:key name="defaultDatabase">main</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="enableDataIntegrityControl">0</s:key>
      <s:key name="enableRealtimeSearch">1</s:key>
      <s:key name="enableTsidxReduction">0</s:key>
      <s:key name="federated.dataset">index:airports-east</s:key>
      <s:key name="federated.provider">FenrisAirNYC</s:key>
      <s:key name="frozenTimePeriodInSecs">188697600</s:key>
      <s:key name="homePath.maxDataSizeMB">0</s:key>
      <s:key name="hotBucketStreaming.deleteHotsAfterRestart">0</s:key>
      <s:key name="hotBucketStreaming.extraBucketBuildingCmdlineArgs"></s:key>
      <s:key name="hotBucketStreaming.removeRemoteSlicesOnRoll">0</s:key>
      <s:key name="hotBucketStreaming.reportStatus">0</s:key>
      <s:key name="hotBucketStreaming.sendSlices">0</s:key>
      <s:key name="hotBucketTimeRefreshInterval">60</s:key>
      <s:key name="indexThreads">auto</s:key>
      <s:key name="journalCompression">gzip</s:key>
      <s:key name="maxConcurrentOptimizes">3</s:key>
      <s:key name="maxDataSize">auto</s:key>
      <s:key name="maxHotBuckets">1</s:key>
      <s:key name="maxHotIdleSecs">0</s:key>
      <s:key name="maxHotSpanSecs">7776000</s:key>
      <s:key name="maxMemMB">5</s:key>
      <s:key name="maxTotalDataSizeMB">500000</s:key>
      <s:key name="maxWarmDBCount">300</s:key>
      <s:key name="memPoolMB">auto</s:key>
      <s:key name="metric.compressionBlockSize">1024</s:key>
      <s:key name="metric.enableFloatingPointCompression">1</s:key>
      <s:key name="metric.maxHotBuckets">1</s:key>
      <s:key name="metric.splitByIndexKeys"></s:key>
      <s:key name="metric.stubOutRawdataJournal">1</s:key>
      <s:key name="metric.timestampResolution">s</s:key>
      <s:key name="metric.tsidxTargetSizeMB">1500</s:key>
      <s:key name="minHotIdleSecsBeforeForceRoll">auto</s:key>
      <s:key name="minStreamGroupQueueSize">2000</s:key>
      <s:key name="quarantineFutureSecs">2592000</s:key>
      <s:key name="quarantinePastSecs">77760000</s:key>
      <s:key name="rawChunkSizeBytes">131072</s:key>
      <s:key name="rotatePeriodInSecs">60</s:key>
      <s:key name="serviceInactiveIndexesPeriod">60</s:key>
      <s:key name="serviceMetaPeriod">1</s:key>
      <s:key name="splitByIndexKeys"></s:key>
      <s:key name="streamingTargetTsidxSyncPeriodMsec">5000</s:key>
      <s:key name="suspendHotRollByDeleteQuery">0</s:key>
      <s:key name="sync">0</s:key>
      <s:key name="timePeriodInSecBeforeTsidxReduction">604800</s:key>
      <s:key name="tsidxDedupPostingsListMaxTermsLimit">8388608</s:key>
      <s:key name="tsidxReductionCheckPeriodInSec">600</s:key>
      <s:key name="tsidxTargetSizeMB">1500</s:key>
      <s:key name="tsidxWritingLevel">1</s:key>
      <s:key name="tstatsHomePath">volume:_splunk_summaries/$_index_name/datamodel_summary</s:key>
    </s:dict>
  </content>
</entry>
```

Example Federated Search for Amazon S3 request and response

Create a new definition for a Federated Search for Amazon S3 federated index named `fss3_index`.

XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/data/federated/index -d
name=federated:fss3_index -d federated.provider=my_federated_provider -d
federated.dataset=aws_glue_table:table_1 -d federated.timefield=field_1 -d federated.timeformat=%25s
```

XML Response

```
<entry>
    <title>federated:fss3_index</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/move" rel="move"/>
    <content type="text/xml">
```

```
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">aws_glue_table:table_1</s:key>
        <s:key name="federated.provider">my_federated_provider</s:key>
        <s:key name="federated.timefield">field_1</s:key>
        <s:key name="federated.timeformat">%s</s:key>
        <s:key name="federated.unixtimefield">_time</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/federated/index/{federated_index_name}

`https://<host>:<mPort>/services/data/federated/provider/{federated_index_name}`

Use this endpoint to:

- Retrieve a specific federated index definition.
- Update a specific federated index definition.
- Delete a specific federated index definition.

Some of these federated index settings are exclusive to Federated Search for Splunk, while others are exclusive to Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform.

For more information about defining federated indexes for Federated Search for Splunk, see Map a federated index to a remote Splunk dataset in *Federated Search.*

For more information about defining federated indexes for Federated Search for Amazon S3, see Map a federated index to an AWS Glue Data Catalog table dataset in *Federated Search*.

Authentication and Authorization
Usage of the POST and DELETE operations for this endpoint is restricted to roles that have the admin_all_objects and indexes_edit **capabilities**.

GET

Returns a definition of a specific `{federated_index_name}`.

Use `federated:{federated_index_name}` for a Federated Search for Splunk federated index. For a Federated Search for Amazon S3 federated index, use `{federated_index_name}`.

Request parameters
None specific to this method. This method can use pagination and filtering parameters.

Returned values
This table is limited to settings specific to federated indexes. For descriptions of other index settings see the entry for `data/indexes`.

> The data/indexes endpoint is available only to users of Splunk Enterprise.

Name	What kinds of federated indexes does this setting apply to?	Description
name	All federated indexes	Specifies the name of the federated index. Uses the syntax `federated:<index_name>`.
federated.provider	All federated indexes	Specifies the federated provider that contains the dataset to which this federated index maps.
federated.dataset	All federated indexes	Specifies the remote dataset on the `federated.provider` to which this federated index maps. Each federated index maps to only one dataset on a federated provider. The dataset is identified by its prefix and name, using the following syntax: `<prefix>:<dataset_name>`. If the `federated.provider` has `type=splunk` in its definition on federated.conf, the possible values for `<prefix>` are `index`, `metricindex`, `savedsearch`, `lastjob`, and `datamodel`. If the `federated.provider` has `type=aws_s3` in its definition on federated.conf, the `<prefix>` must be set to `aws_glue_table`.
federated.timefield	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time field that acts like an event timestamp in the AWS Glue table to which this index maps.
federated.timeformat	Applies only to Federated Search for Amazon S3 federated	Specifies the time format variable or custom time format variable string that matches the `federated.timefield`.

Name	What kinds of federated indexes does this setting apply to?	Description
	indexes	
federated.unixtimefield	Applies only to Federated Search for Amazon S3 federated indexes	An alias for the `federated.timefield` that Splunk software converts into numeric UNIX time format at search time. Insert the `federated.unixtimefield` into federated searches that require numeric UNIX time field values, or when you want to see your time field in numeric UNIX time format in the search results. Defaults to `_time`.
federated.partition.time.fields	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time-related fields in the AWS Glue table to which the index is mapped. Each field is a partition key for a partition time field level indicated by its order in the list. The first field is at the first level, the second field is at the second level, and so on.
federated.partition.time.formats	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time format variables or custom time format strings that correspond to the fields in the `federated.partition.time.fields` list. The first variable corresponds to the first field name, the second variable corresponds to the second field name, and so on.
federated.partition.time.types	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time field types that correspond to the fields in the `federated.partition.time.fields` list. Possible values are `String`, `Integer`, and `Date`.
federated.partition.time.tz	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the timezone that corresponds to the fields in the `federated.partition.time.fields` list. Possible values are canonical timezone names such as `America/Los_Angeles`.

Example Federated Search for Splunk request and response

Return the definition for a Federated Search for Splunk federated index named `remote_index_df_1`.

XML Request

```
curl -k -u admin:changeme -X GET
https://localhost:8126/services/data/federated/index/federated:remote_index_df_1
```

XML response

```
<entry>
    <title>federated:remote_index_df_1</title>
    <id>https://localhost:8126/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1<
/id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">index:index_df_1</s:key>
        <s:key name="federated.provider">provider-1</s:key>
      </s:dict>
    </content>
  </entry>
```

Example Federated Search for Amazon S3 request and response

Return the definition for a Federated Search for Amazon S3 federated index named `fss3_index`.

XML Request

```
curl -k -u admin:changeme -X GET https://localhost:8089/services/data/federated/index/fss3_index
```

XML response

```
<entry>
    <title>federated:fss3_index</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">aws_glue_table:table_1</s:key>
        <s:key name="federated.provider">aws_s3_provider</s:key>
        <s:key name="federated.timefield">field_1</s:key>
        <s:key name="federated.timeformat">%s</s:key>
        <s:key name="federated.unixtimefield">_time</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Updates a definition for a specific `{federated_index_name}`.

Use `federated:{federated_index_name}` for a Federated Search for Splunk federated index. For a Federated Search for Amazon S3 federated index, use `{federated_index_name}`.

These tables are limited to settings specific to federated indexes. For descriptions of other index settings, see the entry for `data/indexes`.

> The data/indexes endpoint is available only to users of Splunk Enterprise.

Request parameters

Name	What kinds of federated indexes does this setting apply to?	Type	Description
federated.timefield	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies the name of a time field that acts like an event timestamp in the AWS Glue table to which this index maps. In other words, the name of the field in the AWS Glue table that behaves like `_time` in the Splunk search processing language. You must provide a `federated.timefield` if you want to use time-related functions to search your remote Amazon S3 data.
federated.timeformat	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies the time format variable or custom time format variable string that matches the `federated.timefield`. The time format variable string must be in Splunk `strptime()` format. This setting is required if you provide a `federated.timefield` value.
federated.unixtimefield	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies an alias for the `federated.timefield` that Splunk software converts into numeric UNIX time format at search time. Insert the `federated.unixtimefield` into federated searches that require numeric UNIX time field values, or when you want to see your time field in numeric UNIX time format in the search results. The `federated.timefield` for a federated index cannot have the same value as the `federated.unixtimefield` for that federated index. In other words, if `federated.timefield` is set to `_time`, you must change the value of `federated.unixtimefield` to a value other than `_time`. Defaults to `_time`.
federated.partition.time.fields	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies a comma-delimited list of time-related fields in your remote data. These fields govern the partitions by which remote data is organized in non-Splunk-platform federated providers (such as Amazon S3 federated providers). Use this setting in conjunction with `federated.partition.time.formats` and `federated.partition.time.types` to identify the hierarchical

Name	What kinds of federated indexes does this setting apply to?	Type	Description
			structure of the data partitions in your remote data. The field list you provide for `federated.partition.time.fields` must correspond with the list of time formats you provide for `federated.partition.time.formats` and the list of data types you provide for `federated.partition.time.types`. Time field names containing comma characters must be surrounded by double quote characters to prevent Splunk software from breaking such values into multiple values. Do not set `federated.partition.time.fields` if the federated provider with which the federated index is associated has `type=splunk`.
federated.partition.time.formats	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies a comma-delimited list of time format variable strings that correspond to the time fields listed by the `federated.partition.time.fields` setting. The '%w'; and '%JT' time format variables are not supported by this setting. See Date and time format variables in the *Search manual*. Time format variable strings containing comma characters must be surrounded by double-quote characters to prevent Splunk software from breaking such strings into multiple values. This setting is required if you have defined a list of `federated.partition.time.fields`. Do not set this setting if `federated.partition.time.fields` is not set.
federated.partition.time.types	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies a comma-delimited list of data type values that correspond to the time fields listed by the `federated.partition.time.fields` setting. The supported time field types are `string`, `integer`, and `date`. This setting is required if you have defined a list of `federated.partition.time.fields`. Do not set this setting if `federated.partition.time.fields` is not set.
federated.partition.time.tz	Applies only to Federated Search for Amazon S3 federated indexes	String	**Optional.** Specifies the time zone to use for the time fields listed in `federated.partition.time.fields`. Use only canonical time zone names such as `America/Los_Angeles`. Do not set this setting if `federated.partition.time.fields` is not set. If this setting is not set when `federated.partition.time.fields` is set, Splunk software uses the per-user time zone, as declared in user-prefs.conf with the `tz`

Name	What kinds of federated indexes does this setting apply to?	Type	Description
			setting.

Returned values

This table is limited to settings specific to federated indexes. For descriptions of other index settings see the entry for `data/indexes`.

The data/indexes endpoint is available only to users of Splunk Enterprise.

Name	What kinds of federated indexes does this setting apply to?	Description
name	All federated indexes	Specifies the name of the federated index. Uses the syntax `federated:<index_name>`.
federated.provider	All federated indexes	Specifies the federated provider that contains the dataset to which this federated index maps.
federated.dataset	All federated indexes	Specifies the remote dataset on the `federated.provider` to which this federated index maps. Each federated index maps to only one dataset on a federated provider. The dataset is identified by its prefix and name, using the following syntax: `<prefix>:<dataset_name>`. If the `federated.provider` has `type=splunk` in its definition on federated.conf, the possible values for `<prefix>` are `index`, `metricindex`, `savedsearch`, `lastjob`, and `datamodel`. If the `federated.provider` has `type=aws_s3` in its definition on federated.conf, the `<prefix>` must be set to `aws_glue_table`.
federated.timefield	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time field in the AWS Glue table to which this index maps that acts like an event timestamp.
federated.timeformat	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the time format variable or custom time format variable string that matches the `federated.timefield`.
federated.unixtimefield	Applies only to Federated Search for Amazon S3 federated indexes	An alias for the `federated.timefield` that Splunk software converts into numeric UNIX time format at search time. Insert the `federated.unixtimefield` into federated searches that require numeric UNIX time field values, or when you want to see your time field in numeric UNIX time format in the search results. Defaults to `_time`.
federated.partition.time.fields		

Name	What kinds of federated indexes does this setting apply to?	Description
	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time-related fields in the AWS Glue table to which the index is mapped. Each field is a partition key for a partition time field level indicated by its order in the list. The first field is at the first level, the second field is at the second level, and so on.
federated.partition.time.formats	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time format variables or custom time format strings that correspond to the fields in the `federated.partition.time.fields` list. The first variable corresponds to the first field name, the second variable corresponds to the second field name, and so on.
federated.partition.time.types	Applies only to Federated Search for Amazon S3 federated indexes	Specifies a comma-delimited list of time field types that correspond to the fields in the `federated.partition.time.fields` list. Possible values are `String`, `Integer`, and `Date`.
federated.partition.time.tz	Applies only to Federated Search for Amazon S3 federated indexes	Specifies the timezone that corresponds to the fields in the `federated.partition.time.fields` list. Possible values are canonical timezone names such as `America/Los_Angeles`.

Example Federated Search for Splunk request and response

Update the dataset mapping for the Federated Search for Splunk `federated:remote_index_df_1` federated index.

XML Request

```
curl -k -u admin:changeme -X POST
https://localhost:8126/services/data/federated/index/federated:remote_index_df_1 -d
federated.dataset=index:index_df_1_new
```

XML response

```
<entry>
    <title>federated:remote_index_df_1</title>
    <id>https://localhost:8126/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1<
/id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Aremote_index_df_1/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">index:index_df_1_new</s:key>
        <s:key name="federated.provider">provider-1</s:key>
      </s:dict>
    </content>
  </entry>
```

Example Federated Search for Amazon S3 request and response

Update the `federated.timefield` for the Federated Search for Amazon S3 `fss3_index` federated index.

XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/data/federated/index/fss3_index -d
federated.timefield=field_2
```

XML response

```
<entry>
    <title>federated:fss3_index</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">aws_glue_table:table_1</s:key>
        <s:key name="federated.provider">test_provider</s:key>
        <s:key name="federated.timefield">field_2</s:key>
        <s:key name="federated.timeformat">%s</s:key>
        <s:key name="federated.unixtimefield">_time</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

DELETE

Deletes a definition for a specific `{federated_index_name}`.

Use `federated:{federated_index_name}` for a Federated Search for Splunk federated index. For a Federated Search for Amazon S3 federated index, use `{federated_index_name}`.

Request parameters
None specific to this method.

Returned values
None specific to this method.

Example Federated Search for Splunk request and response
Delete the `my_federated_index` federated index.

XML Request

```
curl -k -u admin:changeme -X DELETE
https://localhost:8089/services/data/federated/index/federated:my_federated_index
```

XML response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>federated-index</title>
  <id>/services/data/federated/index</id>
  <updated>2021-04-27T12:57:06-07:00</updated>
  <generator build="aa7e77c0d232b8ec1a8c12ceeda95e0bfe3c3f1c" version="20210423"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/index/_new" rel="create"/>
  <link href="/services/data/federated/index/_reload" rel="_reload"/>
  <link href="/services/data/federated/index/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

Example Federated Search for Splunk request and response

Delete the `fss3_index` federated index.

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/data/federated/index/fss3_index
```

XML response

```
<title>federated-index</title>
  <id>https://localhost:8089/services/data/federated/index</id>
  <updated>2024-01-12T16:13:04-08:00</updated>
  <generator build="560faafdef34420e5bda25009961db864cef5986" version="20240110"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/federated/index/_new" rel="create"/>
  <link href="/services/data/federated/index/_reload" rel="_reload"/>
  <link href="/services/data/federated/index/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/federated/index/{federated_index_name}/disable

```
https://<host>:<mPort>/services/data/federated/index/{federated_index_name}/disable
```

Use this endpoint to turn a specific federated index off. When a federated index is turned off, that federated index is not searchable in federated searches. This endpoint applies to federated indexes for Federated Search for Splunk and for Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform deployments.

For more information about defining federated indexes for Federated Search for Splunk, see Map a federated index to a remote Splunk dataset in *Federated Search.*

For more information about defining federated indexes for Federated Search for Amazon S3, see Map a federated index to an AWS Glue Data Catalog table dataset in *Federated Search*.

Authentication and Authorization
Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects **capability**.

POST

Turn off a specific federated index.

Use `federated:{federated_index_name}` for a Federated Search for Splunk federated index. For a Federated Search for Amazon S3 federated index, use `{federated_index_name}`.

Request parameters
None specific to this method.

Returned values
None specific to this method.

Example federated search request and response
Turn off a Federated Search for Amazon S3 index named `fss3_index`.

XML request

```
curl -k -u admin:changeme --request -X POST
https://localhost:8089/services/data/federated/index/fss3_index/disable
```

XML response

```
  <entry>
<title>federated:fss3_index</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
```

```
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">aws_glue_table:table_1</s:key>
        <s:key name="federated.provider">test_provider</s:key>
        <s:key name="federated.timefield">field_1</s:key>
        <s:key name="federated.timeformat">%s</s:key>
        <s:key name="federated.unixtimefield">_time</s:key>
      </s:dict>
    </content>
  </entry>
```

data/federated/index/{federated_index_name}/enable

`https://<host>:<mPort>/services/data/federated/index/{federated_index_name}/enable`

Use this endpoint to turn a federated index back on after you have turned it off. When a federated index is turned on, it can be searched in federated searches. This endpoint applies to federated indexes for Federated Search for Splunk and federated indexes for Federated Search for Amazon S3. Federated Search for Amazon S3 is available only for Splunk Cloud Platform deployments.

For more information about defining federated indexes for Federated Search for Splunk, see Map a federated index to a remote Splunk dataset in *Federated Search.*

For more information about defining federated indexes for Federated Search for Amazon S3, see Map a federated index to an AWS Glue Data Catalog table dataset in *Federated Search*.

Authentication and Authorization

Usage of the POST operation for this endpoint is restricted to roles that have the admin_all_objects **capability**.

POST

Turns a specific federated index on.

Use `federated:{federated_index_name}` for a Federated Search for Splunk federated index. For a Federated Search for Amazon S3 federated index, use `{federated_index_name}`.

Request parameters

None specific to this method.

Returned values

None specific to this method.

Example request and response

Turn on a Federated Search for Amazon S3 federated index named `fss3_index`.

XML request

```
curl -k -u admin:changeme --request -X POST
https://localhost:8089/services/data/federated/index/fss3_index/enable
```

XML response

```
    <entry>
    <title>federated:fss3_index</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="list"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/federated/index/federated%3Afss3_index/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="federated.dataset">aws_glue_table:table_1</s:key>
        <s:key name="federated.provider">test_provider</s:key>
        <s:key name="federated.timefield">field_1</s:key>
        <s:key name="federated.timeformat">%s</s:key>
        <s:key name="federated.unixtimefield">_time</s:key>
      </s:dict>
    </content>
  </entry>
```

Input endpoints

Input endpoint descriptions

Manage and preview streaming and non-streaming and other input data.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

```
https://<deployment-name>.splunkcloud.com:8089
```

Self-service Splunk Cloud deployments
To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

```
https://input-<deployment-name>.cloud.splunk.com:8089
```

See Using the REST API in Splunk Cloud in the the *Splunk REST API Tutorials* for more information.

data/ingest/rfsdestinations

`https://<host>:<mPort>/services/data/ingest/rfsdestinations`
Create/configure, get, or delete an S3 destination for ingest action.

Authentication and authorization

Requires the capabilities `list_ingest_rulesets` and `edit_ingest_rulesets`.

DELETE

Deletes the S3 destination.

Request parameters

Name	Description
name	Name of the S3 destination to delete.

Returned values

Name	Description
name	Name of the S3 destination.
path	Path (bucket and folder) of the destination.
remote.s3.access_key	See indexes.conf.
remote.s3.secret_key	See indexes.conf.
description	Description of the destination (optional).
remote.s3.endpoint	See indexes.conf.
remote.s3.encryption	See indexes.conf.
remote.s3.kms.key_id:	See indexes.conf.
remote.s3.kms.auth_region	See indexes.conf.
remote.s3.signature_version	See indexes.conf.
remote.s3.supports_versioning	See indexes.conf.
remote.s3.url_version	See indexes.conf.
compression	See outputs.conf.
dropEventsOnUploadError	See outputs.conf.
batchTimeout	See outputs.conf.
batchSizeThresholdKB	See outputs.conf.
target	When provided, the request will be proxied to the host specified here (optional).

Example request and response

Request

To delete a destination named a3:

```
curl -v -k -u username:password -X DELETE https://host:port/services/data/ingest/rfsdestinations/a3
```

Response

```
*   Trying 10.140.178.120:9091...

* Connected to mrt (10.140.178.120) port 9091 (#0)

* ALPN, offering h2

* ALPN, offering http/1.1

* successfully set certificate verify locations:

*  CAfile: /etc/ssl/cert.pem

*  CApath: none

* (304) (OUT), TLS handshake, Client hello (1):

* (304) (IN), TLS handshake, Server hello (2):

* TLSv1.2 (IN), TLS handshake, Certificate (11):

* TLSv1.2 (IN), TLS handshake, Server key exchange (12):

* TLSv1.2 (IN), TLS handshake, Server finished (14):

* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):

* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):

* TLSv1.2 (OUT), TLS handshake, Finished (20):

* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):

* TLSv1.2 (IN), TLS handshake, Finished (20):

* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384

* ALPN, server did not agree to a protocol

* Server certificate:

*  subject: CN=SplunkServerDefaultCert; O=SplunkUser

*  start date: May 25 18:24:21 2022 GMT

*  expire date: May 24 18:24:21 2025 GMT

*  issuer: C=US; ST=CA; L=San Francisco; O=Splunk; CN=SplunkCommonCA; emailAddress=support@splunk.com

*  SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.

* Server auth using Basic with user 'admin'

> DELETE /services/data/ingest/rfsdestinations/a3 HTTP/1.1
> Host: mrt:9091

> Authorization: Basic YWRtaW46Y2hhbmdlbWU=

> User-Agent: curl/7.79.1

> Accept: */*

>

* Mark bundle as not supporting multiuse

< HTTP/1.1 200 OK

< Date: Wed, 25 May 2022 20:55:25 GMT

< Expires: Thu, 26 Oct 1978 00:00:00 GMT

< Cache-Control: no-store, no-cache, must-revalidate, max-age=0

< Content-Type: text/xml; charset=UTF-8

< X-Content-Type-Options: nosniff

< Content-Length: 3783

< Vary: Cookie, Authorization

< Connection: Keep-Alive

< X-Frame-Options: SAMEORIGIN

< Server: Splunkd

<

<?xml version="1.0" encoding="UTF-8"?>

<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . .-->

<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

  <title>ingest-rfs-destinations</title>

  <id>https://mrt:9091/services/data/ingest/rfsdestinations</id>

  <updated>2022-05-25T20:55:25+00:00</updated>

  <generator build="fee4ee9be79e70f02f4d13d69c0688e981ab5120" version="20220525"/>
```

```
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/ingest/rfsdestinations/_new" rel="create"/>
<link href="/services/data/ingest/rfsdestinations/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>s3</title>
  <id>https://mrt:9091/services/data/ingest/rfsdestinations/s3</id>
  <updated>1970-01-01T00:00:00+00:00</updated>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="list"/>
  <link href="/services/data/ingest/rfsdestinations/s3/_reload" rel="_reload"/>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="edit"/>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
```

```
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="path">s3://s2-testing-infra/data-action1/sharun/</s:key>
        <s:key name="remote.s3.access_key"><hidden></s:key>
        <s:key name="remote.s3.endpoint">https://s3.us-west-2.amazonaws.com</s:key>
        <s:key name="remote.s3.secret_key"><hidden></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

GET

Gets list of the s3 destination configuration values.

Request parameters

Name	Description
name	Name of the S3 destination. An empty name returns information for all S3 destinations.

Returned values

Name	Description
name	Name of the S3 destination.
path	Path (bucket and folder) of the destination.
remote.s3.access_key	See indexes.conf.
remote.s3.secret_key	See indexes.conf.
description	Description of the destination (optional).
remote.s3.endpoint	See indexes.conf.
remote.s3.encryption	See indexes.conf.
remote.s3.kms.key_id:	See indexes.conf.
remote.s3.kms.auth_region	See indexes.conf.
remote.s3.signature_version	See indexes.conf.
remote.s3.supports_versioning	See indexes.conf.
remote.s3.url_version	See indexes.conf.
compression	See outputs.conf.
dropEventsOnUploadError	See outputs.conf.
batchTimeout	See outputs.conf.
batchSizeThresholdKB	See outputs.conf.
target	When provided, the request will be proxied to the host specified here (optional).

Example request and response

Request

Gets information for destination named "s3":

```
curl -v -k -u username:password https://host:port/services/data/ingest/rfsdestinations/s3
```

Response

```
*   Trying 10.140.178.120:9091...

* Connected to mrt (10.140.178.120) port 9091 (#0)

* ALPN, offering h2

* ALPN, offering http/1.1

* successfully set certificate verify locations:
```

```
*  CAfile: /etc/ssl/cert.pem
*  CApath: none
* (304) (OUT), TLS handshake, Client hello (1):
* (304) (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
* ALPN, server did not agree to a protocol
* Server certificate:
*  subject: CN=SplunkServerDefaultCert; O=SplunkUser
*  start date: May 25 18:24:21 2022 GMT
*  expire date: May 24 18:24:21 2025 GMT
*  issuer: C=US; ST=CA; L=San Francisco; O=Splunk; CN=SplunkCommonCA; emailAddress=support@splunk.com
*  SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
* Server auth using Basic with user 'admin'
> GET /services/data/ingest/rfsdestinations/s3 HTTP/1.1
> Host: mrt:9091
> Authorization: Basic YWRtaW46Y2hhbmdlbWU=
> User-Agent: curl/7.79.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 25 May 2022 20:13:13 GMT
< Expires: Thu, 26 Oct 1978 00:00:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, max-age=0

< Content-Type: text/xml; charset=UTF-8

< X-Content-Type-Options: nosniff

< Content-Length: 5036

< Vary: Cookie, Authorization

< Connection: Keep-Alive

< X-Frame-Options: SAMEORIGIN

< Server: Splunkd

<

<?xml version="1.0" encoding="UTF-8"?>

<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->

<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

  <title>ingest-rfs-destinations</title>

  <id>https://mrt:9091/services/data/ingest/rfsdestinations</id>

  <updated>2022-05-25T20:13:13+00:00</updated>

  <generator build="fee4ee9be79e70f02f4d13d69c0688e981ab5120" version="20220525"/>

  <author>

    <name>Splunk</name>

  </author>

  <link href="/services/data/ingest/rfsdestinations/_new" rel="create"/>

  <link href="/services/data/ingest/rfsdestinations/_reload" rel="_reload"/>

  <opensearch:totalResults>1</opensearch:totalResults>

  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>

  <opensearch:startIndex>0</opensearch:startIndex>

  <s:messages/>
```

```
<entry>
  <title>s3</title>
  <id>https://mrt:9091/services/data/ingest/rfsdestinations/s3</id>
  <updated>1970-01-01T00:00:00+00:00</updated>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="list"/>
  <link href="/services/data/ingest/rfsdestinations/s3/_reload" rel="_reload"/>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="edit"/>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
      <s:item>admin</s:item>
      <s:item>splunk-system-role</s:item>
     </s:list>
    </s:key>
   </s:dict>
  </s:key>
  <s:key name="removable">0</s:key>
  <s:key name="sharing">system</s:key>
 </s:dict>
</s:key>
<s:key name="eai:attributes">
 <s:dict>
  <s:key name="optionalFields">
   <s:list>
    <s:item>authMethod</s:item>
    <s:item>batchSizeThresholdKB</s:item>
    <s:item>batchTimeout</s:item>
    <s:item>compression</s:item>
    <s:item>description</s:item>
    <s:item>dropEventsOnUploadError</s:item>
    <s:item>path</s:item>
    <s:item>remote.s3.access_key</s:item>
    <s:item>remote.s3.encryption</s:item>
    <s:item>remote.s3.endpoint</s:item>
    <s:item>remote.s3.kms.auth_region</s:item>
    <s:item>remote.s3.kms.key_id</s:item>
    <s:item>remote.s3.secret_key</s:item>
    <s:item>remote.s3.signature_version</s:item>
    <s:item>remote.s3.supports_versioning</s:item>
    <s:item>remote.s3.url_version</s:item>
    <s:item>target</s:item>
```

```
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="path">s3://s2-testing-infra/data-action1/sharun/</s:key>
        <s:key name="remote.s3.access_key"><hidden></s:key>
        <s:key name="remote.s3.endpoint">https://s3.us-west-2.amazonaws.com</s:key>
        <s:key name="remote.s3.secret_key"><hidden></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Creates and configures the S3 destination.

Request parameters

Name	Description
name	(Required) Name of the S3 destination.
path	(Required) Path (bucket and folder) of the destination.
remote.s3.access_key	(Optional) See indexes.conf.
remote.s3.secret_key	(Optional) See indexes.conf.
description	(Optional) Description of the destination.
remote.s3.endpoint	(Optional) See indexes.conf.
remote.s3.encryption	(Optional) See indexes.conf.
remote.s3.kms.key_id:	(Optional) See indexes.conf.

Name	Description
remote.s3.kms.auth_region	(Optional) See indexes.conf.
remote.s3.signature_version	(Optional) See indexes.conf.
remote.s3.supports_versioning	(Optional) See indexes.conf.
remote.s3.url_version	(Optional) See indexes.conf.
compression	(Optional) See outputs.conf.
dropEventsOnUploadError	(Optional) See outputs.conf.
batchTimeout	(Optional) See outputs.conf.
batchSizeThresholdKB	(Optional) See outputs.conf.
target	(Optional) When provided, the request will be proxied to the host specified here.

Returned values

Name	Description
name	Name of the S3 destination.
path	Path (bucket and folder) of the destination.
remote.s3.access_key	See indexes.conf.
remote.s3.secret_key	See indexes.conf.
description	Description of the destination.
remote.s3.endpoint	See indexes.conf.
remote.s3.encryption	See indexes.conf.
remote.s3.kms.key_id:	See indexes.conf.
remote.s3.kms.auth_region	See indexes.conf.
remote.s3.signature_version	See indexes.conf.
remote.s3.supports_versioning	See indexes.conf.
remote.s3.url_version	See indexes.conf.
compression	See outputs.conf.
dropEventsOnUploadError	See outputs.conf.
batchTimeout	See outputs.conf.
batchSizeThresholdKB	See outputs.conf.
target	When provided, the request will be proxied to the host specified here (optional).

Example requests and responses

Request

Create a destination with name=s3:

```
curl -v -k -u username:password https://host:port/services/data/ingest/rfsdestinations -d name=s3 -d
```

```
path=s3://s2-testing-infra/data-action1/sharun/ -d remote.s3.access_key=ddd -d remote.s3.secret_key=ddd -d
remote.s3.endpoint=https://s3.us-west-2.amazonaws.com
```

Response

```
*   Trying 10.140.178.120:9091...

* Connected to mrt (10.140.178.120) port 9091 (#0)

* ALPN, offering h2

* ALPN, offering http/1.1

* successfully set certificate verify locations:

*  CAfile: /etc/ssl/cert.pem

*  CApath: none

* (304) (OUT), TLS handshake, Client hello (1):

* (304) (IN), TLS handshake, Server hello (2):

* TLSv1.2 (IN), TLS handshake, Certificate (11):

* TLSv1.2 (IN), TLS handshake, Server key exchange (12):

* TLSv1.2 (IN), TLS handshake, Server finished (14):

* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):

* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):

* TLSv1.2 (OUT), TLS handshake, Finished (20):

* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):

* TLSv1.2 (IN), TLS handshake, Finished (20):

* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384

* ALPN, server did not agree to a protocol

* Server certificate:

*  subject: CN=SplunkServerDefaultCert; O=SplunkUser

*  start date: May 25 18:24:21 2022 GMT

*  expire date: May 24 18:24:21 2025 GMT

*  issuer: C=US; ST=CA; L=San Francisco; O=Splunk; CN=SplunkCommonCA; emailAddress=support@splunk.com

*  SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.

* Server auth using Basic with user 'admin'

> POST /services/data/ingest/rfsdestinations HTTP/1.1

> Host: mrt:9091
> Authorization: Basic YWRtaW46Y2hhbmdlbWU=

> User-Agent: curl/7.79.1

> Accept: */*

> Content-Length: 159

> Content-Type: application/x-www-form-urlencoded

>

* Mark bundle as not supporting multiuse

< HTTP/1.1 201 Created

< Date: Wed, 25 May 2022 20:03:09 GMT

< Expires: Thu, 26 Oct 1978 00:00:00 GMT

< Cache-Control: no-store, no-cache, must-revalidate, max-age=0

< Content-Type: text/xml; charset=UTF-8

< X-Content-Type-Options: nosniff

< Content-Length: 3783

< Vary: Cookie, Authorization

< Connection: Keep-Alive

< X-Frame-Options: SAMEORIGIN

< Server: Splunkd

<

<?xml version="1.0" encoding="UTF-8"?>

<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->

<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

  <title>ingest-rfs-destinations</title>

  <id>https://mrt:9091/services/data/ingest/rfsdestinations</id>

  <updated>2022-05-25T20:03:09+00:00</updated>
```

```
<generator build="fee4ee9be79e70f02f4d13d69c0688e981ab5120" version="20220525"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/ingest/rfsdestinations/_new" rel="create"/>
<link href="/services/data/ingest/rfsdestinations/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>s3</title>
  <id>https://mrt:9091/services/data/ingest/rfsdestinations/s3</id>
  <updated>1970-01-01T00:00:00+00:00</updated>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="list"/>
  <link href="/services/data/ingest/rfsdestinations/s3/_reload" rel="_reload"/>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="edit"/>
  <link href="/services/data/ingest/rfsdestinations/s3" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
```

```
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="path">s3://s2-testing-infra/data-action1/sharun/</s:key>
        <s:key name="remote.s3.access_key"><hidden></s:key>
        <s:key name="remote.s3.endpoint">https://s3.us-west-2.amazonaws.com</s:key>
        <s:key name="remote.s3.secret_key"><hidden></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```
===========================
```

Note also that this action will create an `outputs.conf` file with the following stanza:

```
[rfs:s3]

path = s3://s2-testing-infra/data-action1/sharun/

remote.s3.access_key = $7$F2Amvz3gXvMdCAX9p8RKwjdWKItSkSRakj9G2ZmULuWkccs= (encrypted)

remote.s3.endpoint = https://s3.us-west-2.amazonaws.com

remote.s3.secret_key = $7$AL6QuynbFGdNQu5dwh6puzt9dSFXDKdQn6ypEhVjxz0feAI= (encrypted)
```

Request
Edit a destination:

```
curl -v -k -u username:password https://host:port/services/data/ingest/rfsdestinations/s3 -d
path=s3://s2-testing-infra/data-action1/sharun100/-d remote.s3.access_key=aaa -d remote.s3.secret_key=bbb
-d remote.s3.endpoint=https://s3.us-west-2.amazonaws.com
```

Response

```
 *   Trying 10.140.178.120:9011...

* TCP_NODELAY set

* Connected to mrt (10.140.178.120) port 9011 (#0)

* ALPN, offering h2

* ALPN, offering http/1.1

* successfully set certificate verify locations:

*   CAfile: /etc/ssl/certs/ca-certificates.crt

  CApath: /etc/ssl/certs

* TLSv1.3 (OUT), TLS handshake, Client hello (1):

* TLSv1.3 (IN), TLS handshake, Server hello (2):

* TLSv1.2 (IN), TLS handshake, Certificate (11):

* TLSv1.2 (IN), TLS handshake, Server key exchange (12):

* TLSv1.2 (IN), TLS handshake, Server finished (14):

* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):

* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):

* TLSv1.2 (OUT), TLS handshake, Finished (20):

* TLSv1.2 (IN), TLS handshake, Finished (20):

* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384

* ALPN, server did not agree to a protocol
* Server certificate:
*  subject: CN=SplunkServerDefaultCert; O=SplunkUser
*  start date: May 10 22:10:51 2022 GMT
*  expire date: May  9 22:10:51 2025 GMT
*  issuer: C=US; ST=CA; L=San Francisco; O=Splunk; CN=SplunkCommonCA; emailAddress=support@splunk.com
*  SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
* Server auth using Basic with user 'admin'
> POST /services/data/ingest/rfsdestinations/s3 HTTP/1.1
> Host: mrt:9011
> Authorization: Basic YWRtaW46Y2hhbmdlbWU=
> User-Agent: curl/7.68.0
> Accept: */*
> Content-Length: 208
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 208 out of 208 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 31 May 2022 19:01:37 GMT
< Expires: Thu, 26 Oct 1978 00:00:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, max-age=0
< Content-Type: text/xml; charset=UTF-8
< X-Content-Type-Options: nosniff
< Content-Length: 3786
< Vary: Cookie, Authorization
< Connection: Keep-Alive
< X-Frame-Options: SAMEORIGIN
< Server: Splunkd
<
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . .
```

```
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . .-->

<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

  <title>ingest-rfs-destinations</title>

  <id>https://mrt:9011/services/data/ingest/rfsdestinations</id>

  <updated>2022-05-31T19:01:37+00:00</updated>

  <generator build="d7f338ee11f8c6ff9ba4e4d98ff6e9b1b8da6a9c" version="20220510"/>

  <author>

    <name>Splunk</name>

  </author>

  <link href="/services/data/ingest/rfsdestinations/_new" rel="create"/>

  <link href="/services/data/ingest/rfsdestinations/_reload" rel="_reload"/>

  <opensearch:totalResults>1</opensearch:totalResults>

  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>

  <opensearch:startIndex>0</opensearch:startIndex>

  <s:messages/>

  <entry>

    <title>s3</title>

    <id>https://mrt:9011/services/data/ingest/rfsdestinations/s3</id>

    <updated>1970-01-01T00:00:00+00:00</updated>

    <link href="/services/data/ingest/rfsdestinations/s3" rel="alternate"/>

    <author>

      <name>system</name>

    </author>

    <link href="/services/data/ingest/rfsdestinations/s3" rel="list"/>

    <link href="/services/data/ingest/rfsdestinations/s3/_reload" rel="_reload"/>

    <link href="/services/data/ingest/rfsdestinations/s3" rel="edit"/>
```

```
<link href="/services/data/ingest/rfsdestinations/s3" rel="remove"/>
<content type="text/xml">
  <s:dict>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="path">s3://s2-testing-infra/data-action1/sharun100/</s:key>
```

```
        <s:key name="remote.s3.access_key"><hidden></s:key>

        <s:key name="remote.s3.endpoint">https://s3.us-west-2.amazonaws.com</s:key>

        <s:key name="remote.s3.secret_key"><hidden></s:key>

      </s:dict>

    </content>

  </entry>

</feed>
```

Request

Test connection to destination:

```
curl -v -k -u username:password https://host:port/services/data/ingest/rfsdestinations/a3/test -d
path=s3://s2-testing-infra/data-action1/sharun/-d remote.s3.access_key=aaa -d remote.s3.secret_key=bbb -d
remote.s3.endpoint=https://s3.us-west-2.amazonaws.com
```

Response

```
 *   Trying 10.140.178.120:9011...

* TCP_NODELAY set

* Connected to mrt (10.140.178.120) port 9011 (#0)

* ALPN, offering h2

* ALPN, offering http/1.1

* successfully set certificate verify locations:

*   CAfile: /etc/ssl/certs/ca-certificates.crt

  CApath: /etc/ssl/certs

* TLSv1.3 (OUT), TLS handshake, Client hello (1):

* TLSv1.3 (IN), TLS handshake, Server hello (2):

* TLSv1.2 (IN), TLS handshake, Certificate (11):

* TLSv1.2 (IN), TLS handshake, Server key exchange (12):

* TLSv1.2 (IN), TLS handshake, Server finished (14):

* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):

* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):

* TLSv1.2 (OUT), TLS handshake, Finished (20):

* TLSv1.2 (IN), TLS handshake, Finished (20):
```

```
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384

* ALPN, server did not agree to a protocol

* Server certificate:

*  subject: CN=SplunkServerDefaultCert; O=SplunkUser

*  start date: May 10 22:10:51 2022 GMT

*  expire date: May  9 22:10:51 2025 GMT

*  issuer: C=US; ST=CA; L=San Francisco; O=Splunk; CN=SplunkCommonCA; emailAddress=support@splunk.com

*  SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.

* Server auth using Basic with user 'admin'

> POST /services/data/ingest/rfsdestinations/a3/test HTTP/1.1

> Host: mrt:9011

> Authorization: Basic YWRtaW46Y2hhbmdlbWU=

> User-Agent: curl/7.68.0

> Accept: */*

> Content-Length: 205

> Content-Type: application/x-www-form-urlencoded

>

* upload completely sent off: 205 out of 205 bytes

* Mark bundle as not supporting multiuse

< HTTP/1.1 200 OK

< Date: Tue, 31 May 2022 19:07:32 GMT

< Expires: Thu, 26 Oct 1978 00:00:00 GMT

< Cache-Control: no-store, no-cache, must-revalidate, max-age=0

< Content-Type: text/xml; charset=UTF-8

< X-Content-Type-Options: nosniff

< Content-Length: 1998

< Vary: Cookie, Authorization

< Connection: Keep-Alive

< X-Frame-Options: SAMEORIGIN

< Server: Splunkd

<
```

```
<?xml version="1.0" encoding="UTF-8"?>

<!--This is to override browser formatting; see server.conf[httpServer] to disable. . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . .-->

<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

  <title>ingest-rfs-destinations</title>

  <id>https://mrt:9011/services/data/ingest/rfsdestinations</id>

  <updated>2022-05-31T19:07:32+00:00</updated>

  <generator build="d7f338ee11f8c6ff9ba4e4d98ff6e9b1b8da6a9c" version="20220510"/>

  <author>

    <name>Splunk</name>

  </author>

  <link href="/services/data/ingest/rfsdestinations/_new" rel="create"/>

  <link href="/services/data/ingest/rfsdestinations/_reload" rel="_reload"/>

  <opensearch:totalResults>0</opensearch:totalResults>

  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>

  <opensearch:startIndex>0</opensearch:startIndex>

  <s:messages>

    <s:msg type="INFO">The given s3/s3-supported destination and credentials are valid.</s:msg>

  </s:messages>

</feed>
```

data/ingest/rulesets

`https://<host>:<mPort>/services/data/ingest/rulesets`

Retrieve a list of your rulesets.

GET

Return a list of your deployed rulesets.

Request parameters
None

Returned values

Name	Description
Name	The name of the retrieved ruleset.
Sourcetype	The sourcetype of the deployed ruleset.
Rules	The rules for your deployed ruleset.

Example request and response.

JSON Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/ingest/rulesets\?output_mode\=json
```

JSON Encoded Response

```
{"links":{},"entry":[{"name":"audittrail_to_s3","content":{"name":"audittrail_to
_s3","description":"","sourcetype":"audittrail","rules":[{"name":"fgf5emvw","action":"filter_regex","field":"
_raw","match":"lis"},{"name":"ripxbt8o","action":"route_regex","dest":"rfs:s3","field":"
_raw","match":"acc"}]}},{"name":"ruleset1","content":{"name":"ruleset1","description":"","sourcetype":"foo1","
rules":[]}},{"name":"ruleset_splunkd_ui_access","content":{"name":"ruleset_splunkd_ui
_access","description":"x","sourcetype":"splunkd_ui_access","rules":[{"name":"f3kbymjc","action":"filter
_regex","field":"_raw","match":"server/health"}]}}]}%
```

POST

Creates and updates a ruleset.

Request parameters

Name	Description
Name	The name of the retrieved ruleset.
Sourcetype	The sourcetype of the deployed ruleset.
Rules	The rules for your deployed ruleset.

Returned values

Name	Description
Name	The name of the retrieved ruleset.
Sourcetype	The sourcetype of the deployed ruleset.
Rules	The rules for your deployed ruleset.

Example request and response.

JSON Request

```
curl -k -u admin:changeme -X POST -d name=hello1 -d sourcetype=foobar1 -d
'rules=[{"name":"r1","action":"filter_regex","match":"hello"}]'
https://localhost:8089/services/data/ingest/rulesets\?output_mode\=json
```

JSON Encoded Response

```
{"links":{},"entry":[{"name":"audittrail_to_s3","content":{"name":"audittrail_to
_s3","description":"","sourcetype":"audittrail","rules":[{"name":"fgf5emvw","action":"filter_regex","field":"
_raw","match":"lis"},{"name":"ripxbt8o","action":"route_regex","dest":"rfs:s3","field":"
_raw","match":"acc"}]}},{"name":"ruleset1","content":{"name":"ruleset1","description":"","sourcetype":"foo1","
rules":[]}},{"name":"ruleset_splunkd_ui_access","content":{"name":"ruleset_splunkd_ui
_access","description":"x","sourcetype":"splunkd_ui_access","rules":[{"name":"f3kbymjc","action":"filter
_regex","field":"_raw","match":"server/health"}]}}]}%
```

data/ingest/rulesets/{name}

```
https://<host>:<mPort>/services/data/ingest/rulesets/{name}
```

Retrieve a particular ruleset.

GET

Return a named deployed ruleset.

Request parameters

None

Returned values

Name	Description
Name	The name of the retrieved ruleset.
Sourcetype	The sourcetype of the deployed ruleset.
Rules	The rules for your deployed ruleset.

Example request and response.

JSON Request

```
GET /data/ingest/rulesets?output_mode=json
```

JSON Encoded Response

```
{
    name: "Drop security data",
    sourcetype: "syslog",
    rules: [
        { name: "Security - rarely important",
          match: "Kerberos service ticket was (requested|renewed)",
          action: "filter_regex"
        } ]
}
```

POST

Creates and updates a named ruleset.

Request parameters

Name	Description
Name	The name of the retrieved ruleset.
Match	What your deployed ruleset matches.
Action	The action that your deployed ruleset does.

Returned values

Name	Description
Name	The name of the retrieved ruleset.
Match	What your deployed ruleset matches.
Action	The action that your deployed ruleset does.

Example request and response.

JSON Request

```
curl -k -u admin:Chang3d! https://localhost:8089/services/data/ingest/rulesets?output_mode=json -d
name=ruleset1 -d sourcetype=splunkd_access -d rules="[{\"name\": \"rule1\", \"cond\": {\"type\": \"regex\",
\"field\": \"_raw\", \"match\": \"DEBUG\"}, \"action\": \"filter\"}]"
```

JSON Encoded Response

```
{
  "links": {},
  "entry": [
    {
      "name": "hello1",
      "content": {
        "name": "hello1",
        "description": "",
        "sourcetype": "foobar1",
        "rules": [
          {
            "name": "r1",
            "action": "filter_regex",
            "field": "_raw",
            "match": "hello"
          }
        ]
      }
    }
  ]
}
```

data/ingest/rulesets/publish

```
https://<host>:<mPort>/services/data/ingest/rulesets/publish
```

Publish ruleset changes on the indexer cluster manager.

POST

Push the ruleset changes into deployment.

Request parameters

None

Returned values

Name	Description
Name	The name of the retrieved ruleset.
Match	What your deployed ruleset matches.
Action	The action that your deployed ruleset does.

Example request and response.

JSON Request

```
curl -k -u admin:changeme -X POST -d 'rules=[{"name":"r1","action":"filter_regex","match":"hello"}]'
https://localhost:8089/services/data/ingest/rulesets/hello1\?output_mode\=json
```

JSON Encoded Response

```
{
  "messages": [
    {
      "status": "succeeded",
      "new_checksum": "B4D4DB74DD2BF50AD9D51F999E3EBBAD"
    }
  ]
}
```

data/inputs/ad

```
https://<host>:<mPort>/services/data/inputs/ad
```

Access and configure the active directory monitoring input.

GET

Get the current active directory monitoring configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
disabled	Indicates whether this input is disabled.
index	The index in which to store the gathered data. If no value is present, sends data to the default index.
monitorSubtree	Indicates whether or not to monitor the subtrees of a given Active Directory tree path.
startingNode	Tells Splunk software where in the Active Directory directory tree to start monitoring. If not specified, Splunk software attempts to start at the root of the directory tree. The user as which you configure Splunk to run at installation determines where Splunk software starts monitoring.
targetDc	Fully qualified domain name of a valid, network-accessible Active Directory domain controller. If not specified, Splunk software obtains the local computer DC by default, and binds to its root Distinguished Name (DN).

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/ad
```

XML Response

```
...
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/services/data/inputs/ad</id>
  <updated>2011-07-29T19:13:28-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/ad/_new" rel="create"/>
  <link href="/services/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>NearestDC</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/ad/NearestDC</id>
    <updated>2011-07-29T19:13:28-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC" rel="edit"/>
    <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC/enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="index">default</s:key>
        <s:key name="monitorSubtree">1</s:key>
        <s:key name="startingNode"/>
        <s:key name="targetDc"/>
      </s:dict>
    </content>
  </entry>
```

POST

Create or modify performance monitoring settings.

Request parameters

Name	Datatype	Default	Description
baseline	Boolean		Indicates whether to query baseline objects. Defaults to true. Baseline objects are objects which currently reside in Active Directory and include previously deleted objects.
host	String	Docs-W8R2-Std7	Host name for the Active Directory Monitor.
index	String	default	The index in which to store the gathered data. If not specified defaults to the default index.
monitorSubtree	Number		**Required**. Whether or not to monitor the subtree(s) of a given directory tree path. 1 means yes, 0 means no.
name	String		**Required**. A unique name that represents a configuration or set of configurations for a specific domain controller.
printSchema	Boolean		Indicates whether to print the Active Directory schema. Defaults to true.
source	String		Source for data inputs.
sourcetype	String		Source type of data inputs.
startingNode	String		Where in the Active Directory directory tree to start monitoring. If not specified, attempts to start at the root of the directory tree.
targetDc	String		Specifies a fully qualified domain name of a valid, network-accessible domain controller. If not specified, Splunk software gets the local domain controller.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/admin/search/data/inputs/ad -d monitorSubtree=0 -d
name=newdc
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</id>
  <updated>2011-07-29T19:14:57-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/ad/{name}

`https://<host>:<mPort>/services/data/inputs/ad/{name}`

Manage `{name}` active directory monitoring.

DELETE

Delete the `{name}` Active Directory monitoring stanza.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/ad/newdc
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</id>
  <updated>2011-07-29T19:22:50-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Gets the current configuration for the `{name}` Active Directory monitoring stanza.

Request parameters

None

Returned values

Name	Description
Attribute	**Description**
disabled	Indicates whether this input is disabled.
index	The index in which to store the gathered data. If no value is present, send data to the default index.
monitorSubtree	Indicates whether or not to monitor the subtrees of a given Active Directory tree path.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/ad/newdc
```

XML Response

```
...
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</id>
  <updated>2011-07-29T19:18:18-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>newdc</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad/newdc</id>
    <updated>2011-07-29T19:18:18-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/ad/newdc" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/ad/newdc" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/ad/newdc/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/ad/newdc" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/ad/newdc" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/ad/newdc/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>disabled</s:item>
                <s:item>index</s:item>
                <s:item>startingNode</s:item>
                <s:item>targetDc</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>monitorSubtree</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="index">default</s:key>
        <s:key name="monitorSubtree">0</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update the `{name}` Active Directory monitoring stanza.

Request parameters

Name	Datatype	Default	Description

baseline	Boolean		Indicates whether to query baseline objects. Defaults to true. Baseline objects are objects which currently reside in Active Directory and include previously deleted objects.
host	String	Docs-W8R2-Std7	Host name for the Active Directory Monitor.
index	String	default	The index in which to store the gathered data. If not specified defaults to the default index.
monitorSubtree required	Number		Whether or not to monitor the subtree(s) of a given directory tree path. 1 means yes, 0 means no.
printSchema	Boolean		Indicates whether to print the Active Directory schema. Defaults to true.
source	String		Source for data inputs.
sourcetype	String		Source type of data inputs.
startingNode	String		Where in the Active Directory directory tree to start monitoring. If not specified, attempts to start at the root of the directory tree.
targetDc	String		Specifies a fully qualified domain name of a valid, network-accessible DC. If not specified, Splunk software gets the local computer's DC.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/ad/newdc -d monitorSubtree=1
```

XML Response

```
...
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</id>
  <updated>2011-07-29T19:20:16-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
```

data/inputs/all

```
https://<host>:<mPort>/services/data/inputs/all
```

Access all inputs to the Splunk deployment. This includes any modular inputs that may be defined on the system.

GET

List all inputs, including modular inputs.

Request parameters

Name	Datatype	Description
common	Boolean	Indicates whether to return only attributes common to all inputs. The common attributes are as follows. • app • disabled • host • index • owner • source • sourcetype • title • updated

Pagination and filtering parameters can be used with this method.

Returned values

Returns an `<entry>` element for each input, listing attributes specific to the input. See the following example for more details.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/all
```

XML Response

```
...
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>all</title>
  <id>https://localhost:8089/services/data/inputs/all</id>
  <updated>2012-10-01T16:08:24-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/all/_new" rel="create"/>
  <link href="/services/data/inputs/all/_reload" rel="_reload"/>
  <link href="/services/data/inputs/all/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title></title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/all/</id>
    <updated>2012-10-01T16:08:24-07:00</updated>
    <link href="/servicesNS/nobody/system/data/inputs/all/" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/inputs/all/" rel="list"/>
    <link href="/servicesNS/nobody/system/data/inputs/all//_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/inputs/all/" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/inputs/all//enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="cipherSuite">ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="host">splunks-ombra.sv.splunk.com</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>$SPLUNK_HOME/etc/splunk.version</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/all/%24SPLUNK
_HOME%252Fetc%252Fsplunk.version</id>
    <updated>2012-10-01T16:08:24-07:00</updated>
    <link href="/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version"
rel="list"/>
    <link href="/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version"
rel="edit"/>
    <link href="/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_TCP_ROUTING">*</s:key>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="filecount">1</s:key>
        <s:key name="host">splunks-ombra.sv.splunk.com</s:key>
        <s:key name="index">_internal</s:key>
        <s:key name="sourcetype">splunk_version</s:key>
      </s:dict>
    </content>
  </entry>
   . . . elided ...
```

data/inputs/all/{name}

`https://<host>:<mPort>/services/data/inputs/all/{name}`

Get information about the `{name}` input source.

GET

List details for the `{name}` input.

Request parameters

Name	Datatype	Description
common	Boolean	Indicates whether to return only attributes common to all inputs. These common attributes are as follows. • `app` • `disabled` • `host` • `index` • `owner` • `source` • `sourcetype` • `title` • `updated`

Returned values

The response lists attributes for the `{name}` input. See the following example for details.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/all/twitter
```

XML Response

```
...
 <title>all</title>
  <id>https://localhost:8089/services/data/inputs/all</id>
  <updated>2012-07-11T08:03:17-07:00</updated>
  <generator build="129290" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/all/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>twitter</title>
    <id>https://localhost:8089/services/data/inputs/all/twitter</id>
    <updated>2012-07-11T08:03:17-07:00</updated>
    <link href="/services/data/inputs/all/twitter" rel="alternate"/>
    <author>
```

```
      <name>system</name>
    </author>
    <link href="/services/data/inputs/all/twitter" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description">Get data from Twitter.</s:key>
        ... eai:acl nodes and eai:attribute nodes elided ...
        <s:key name="endpoint">
          <s:dict>
            <s:key name="args">
              <s:dict>
                <s:key name="name">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Name of the current feed using the user credentials
supplied.</s:key>
                    <s:key name="order">0</s:key>
                    <s:key name="title">Twitter feed name</s:key>
                  </s:dict>
                </s:key>
                <s:key name="password">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Your twitter password</s:key>
                    <s:key name="order">2</s:key>
                    <s:key name="required_on_create">1</s:key>
                    <s:key name="required_on_edit">0</s:key>
                    <s:key name="title">Password</s:key>
                  </s:dict>
                </s:key>
                <s:key name="username">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Your Twitter ID.</s:key>
                    <s:key name="order">1</s:key>
                    <s:key name="required_on_create">1</s:key>
                    <s:key name="required_on_edit">0</s:key>
                    <s:key name="title">Twitter ID/Handle</s:key>
                  </s:dict>
                </s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="streaming_mode">simple</s:key>
        <s:key name="title">Twitter</s:key>
      </s:dict>
    </content>
  </entry>
```

data/inputs/http

`https://<host>:<mPort>/services/data/inputs/http`

Access or update HTTP Event Collector global configuration tokens and application tokens.

See also

For more information, see details for the following associated endpoints.

- data/inputs/http/{name}
- data/inputs/http/{name}/enable
- data/inputs/http/{name}/disable
- collector/event

GET

Access global configuration information and a list of tokens

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

See `data/inputs/http/{name}` for app-level response data keys.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/http
```

XML Response

```
 <title>http</title>
 <id>https://localhost:8089/services/data/inputs/http</id>
 <updated>2015-01-26T22:43:26-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/inputs/http/_new" rel="create"/>
 <link href="/services/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch elided ...
 <s:messages/>
 <entry>
   <title>http</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http</id>
   <updated>2015-01-26T22:43:26-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/inputs/http/http" rel="list"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http/disable" rel="disable"/>
   <content type="text/xml">
```

```
     <s:dict>
       <s:key name="_rcvbuf">1572864</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl elided ...
       <s:key name="eai:appName">search</s:key>
       <s:key name="eai:userName">admin</s:key>
       <s:key name="host">$decideOnStartup</s:key>
       <s:key name="index">default</s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>http://%22myapp"</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22</id>
   <updated>2015-01-26T22:43:26-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="alternate"/>
   <author>
     <name>admin</name>
   </author>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="list"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/disable"
rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="_rcvbuf">1572864</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl elided ...
       <s:key name="eai:appName">search</s:key>
       <s:key name="eai:userName">admin</s:key>
       <s:key name="host">$decideOnStartup</s:key>
       <s:key name="index">default</s:key>
       <s:key name="token">3DEA16E1-413A-46C2-A74F-E79DC3DF3CA2</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Modify global configuration. Add and modify tokens.

Global request parameters

Name	Datatype	Default	Description
dedicatedIoThreads	Number	`2`	Number of threads used by HTTP Input server.
disabled	Boolean	`1`	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
enableSSL	Boolean	`1`	Enable SSL protocol for HTTP data input. `1` = SSL enabled, `0` = SSL disabled.
index	String		Index to store generated events.
indexes	String		Set of indexes allowed for events with this token.

Name	Datatype	Default	Description
maxSockets	Number	0	Maximum number of simultaneous HTTP connections accepted. Adjusting this value may cause server performance issues and is not generally recommended. Possible values for this setting vary by OS.
maxThreads	Number	0	Maximum number of threads that can be used by active HTTP transactions. Adjusting this value may cause server performance issues and is not generally recommended. Possible values for this setting vary by OS.
name required	String		Token name (`inputs.conf` key)
port	Number	8088	HTTP data input IP port.
source	String		Default source for events with this token.
sourcetype	String		Default sourcetype for events with this token.
useDeploymentServer	Boolean	`0` (disabled)	Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to `1` (enabled), the input writes its configuration to the directory specified as `repositoryLocation` in `serverclass.conf`. Copy the full contents of the `splunk_httpinput` app directory to this directory for the configuration to work. When enabled, only the tokens defined in the `splunk_httpinput` app in this repository are viewable and editable on the **API and the Data Inputs** page in Splunk Web. When disabled, the input writes its configuration to `$SPLUNK_HOME/etc/apps` by default. Defaults to 0 (disabled).

Application-level request parameters

Name	Datatype	Default	Description
disabled	Boolean	`1`	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
index	String		Index to store generated events.
indexes	String		Set of indexes allowed for events with this token.
name required	String		Token name (`inputs.conf` key)
source	String		Default source for events with this token.
sourcetype	String		Default sourcetype for events with this token.

Global returned values

Name	Description
dedicatedIoThreads	

Name	Description		
	Number of threads used by HTTP Input server.		
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.		
enableSSL	Enable SSL protocol for HTTP data input. `1` = SSL enabled, `0` = SSL disabled.		
host	Host from which the indexer gets data.		
index	Index to store generated events.		
indexes	Set of indexes allowed for events with this token.		
port	HTTP data input IP port.		
_rcvbuf	Socket receive buffer size (bytes).		
source	Default source for events with this token.		
sourcetype	Default sourcetype for events with this token.		
useDeploymentServer	Boolean	`0` (disabled)	Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to `1` (enabled), the input writes its configuration to the directory specified as `repositoryLocation` in `serverclass.conf`. Copy the full contents of the `splunk_httpinput` app directory to this directory for the configuration to work. When enabled, only the tokens defined in the `splunk_httpinput` app in this repository are viewable and editable on the **API and the Data Inputs** page in Splunk Web. When disabled, the input writes its configuration to `$SPLUNK_HOME/etc/apps` by default. Defaults to 0 (disabled).

Application-level returned values

Name	Description
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.

Name	Description
host	Host from which the indexer gets data.
index	Index to store generated events.
_rcvbuf	Socket receive buffer size (bytes).
source	Source for events with this token.
sourcetype	Sourcetype for events with this token.
token	Token value for sending data to `collector/event` endpoint.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/http -d name=myapp
```

XML Response

```
...
 <title>http</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
 <updated>2015-01-30T12:45:28-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
 <link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch ...
 <s:messages/>
 <entry>
   <title>http://myapp</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp</id>
   <updated>2015-01-30T12:45:28-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="list"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="_rcvbuf">1572864</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl ...
       <s:key name="eai:appName">system</s:key>
       <s:key name="eai:userName">nobody</s:key>
       <s:key name="host">$decideOnStartup</s:key>
       <s:key name="index">default</s:key>
       <s:key name="token">AABD8B82-2810-4BE8-823F-FE6C15ECB46E</s:key>
     </s:dict>
   </content>
 </entry>
```

data/inputs/http/{name}

```
https://<host>:<mPort>/services/data/inputs/http/{name}
```

Manage the `{name}` HTTP Event Collector token. `HTTP`, as in `data/inputs/http/http`, indicates global configuration.

See also

For more information, see details for the following associated endpoints.

- data/inputs/http
- data/inputs/http/{name}/enable
- data/inputs/http/{name}/disable
- collector/event

DELETE

Delete a token.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%3A%252F%252Fmyapp
```

XML Response

```
 <title>http</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
 <updated>2015-01-30T13:03:18-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
 <link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch elided ...
 <s:messages/>
</feed>
```

GET

Get token configuration details.

Request parameters
None

Global response data keys

Name	Description
_rcvbuf	Socket receive buffer size (bytes).
dedicatedIoThreads	Number of threads for HTTP event collector server.
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
enableSSL	SSL enablement status.
host	Host from which the indexer gets data.
index	Index to store generated events.
port	HTTP data event collector IP port.
source	Source for events with this token.
sourcetype	Sourcetype for events with this token.
token	Token value for sending data to `collector/event` endpoint.
useDeploymentServer	Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to `1` (enabled), the input writes its configuration to the directory specified as `repositoryLocation` in `serverclass.conf`. Copy the full contents of the `splunk_httpinput` app directory to this directory for the configuration to work. When enabled, only the tokens defined in the `splunk_httpinput` app in this repository are viewable and editable on the **API and the Data Inputs** page in Splunk Web. When disabled, the input writes its configuration to `$SPLUNK_HOME/etc/apps` by default. Defaults to 0 (disabled).

Application-level response data keys

Name	Description
_rcvbuf	Socket receive buffer size (bytes).

Name	Description
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	Host from which the indexer gets data.
index	Index to store generated events.
source	Source for events with this token.
sourcetype	Sourcetype for events with this token.
token	Token value for sending data to `collector/event` endpoint.

Example request and response

XML Request

```
curl -u admin:pass
https://localhost:8089//servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/http
/%252Fvar%252Flog
```

XML Response

```
...
 <title>http</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
 <updated>2015-01-26T23:01:34-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
 <link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch elided ...
 <s:messages/>
 <entry>
   <title>http://%22myapp"</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22</id>
   <updated>2015-01-26T23:01:34-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="alternate"/>
   <author>
     <name>admin</name>
   </author>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="list"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/disable"
rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="_rcvbuf">1572864</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl elided ...
       <s:key name="eai:appName">system</s:key>
```

```
      ... eai:attributes elided ...
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="host">$decideOnStartup</s:key>
      <s:key name="index">default</s:key>
      <s:key name="token">3DEA16E1-413A-46C2-A74F-E79DC3DF3CA2</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update token configuration information.

Request parameters

Name	Datatype	Default	Description
disabled	Boolean	`1`	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	String		Default host.
index	String		Index to store generated events.
indexes	String		Set of indexes allowed for events with this token.
name	String		**Required**. Token name (`inputs.conf` key)
source	String		Default source for events with this token.
sourcetype	String		Default sourcetype for events with this token.
useDeploymentServer	Boolean	`0` (disabled)	Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to `1` (enabled), the input writes its configuration to the directory specified as `repositoryLocation` in `serverclass.conf`. Copy the full contents of the `splunk_httpinput` app directory to this directory for the configuration to work. When enabled, only the tokens defined in the `splunk_httpinput` app in this repository are viewable and editable on the **API and the Data Inputs** page in Splunk Web. When disabled, the input writes its configuration to `$SPLUNK_HOME/etc/apps` by default. Defaults to 0 (disabled).

Returned values

Name	Description
_rcvbuf	Socket receive buffer size (bytes).

Name	Description
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	Host from which the indexer gets data.
index	Index to store generated events.
source	Source for events with this token.
sourcetype	Sourcetype for events with this token.
token	Token value for sending data to `collector/event` endpoint.
useDeploymentServer	Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to `1` (enabled), the input writes its configuration to the directory specified as `repositoryLocation` in `serverclass.conf`. Copy the full contents of the `splunk_httpinput` app directory to this directory for the configuration to work. When enabled, only the tokens defined in the `splunk_httpinput` app in this repository are viewable and editable on the **API and the Data Inputs** page in Splunk Web. When disabled, the input writes its configuration to `$SPLUNK_HOME/etc/apps` by default. Defaults to 0 (disabled).

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/http%3A%252F%252Fmyapp -d
recursive=false
```

XML Response

```
...
 <title>http</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
 <updated>2015-01-30T12:51:17-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
 <link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch elided ...
 <s:messages/>
 <entry>
   <title>http://myapp</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp</id>
   <updated>2015-01-30T12:51:17-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="alternate"/>
   <author>
```

```
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="list"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="remove"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="_rcvbuf">1572864</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl elided ...
      <s:key name="eai:appName">system</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="host">$decideOnStartup</s:key>
      <s:key name="index">default</s:key>
      <s:key name="recursive">false</s:key>
      <s:key name="token">AABD8B82-2810-4BE8-823F-FE6C15ECB46E</s:key>
    </s:dict>
  </content>
</entry>
```

data/inputs/http/{name}/disable

`https://<host>:<mPort>/services/data/inputs/http/{name}/disable`

Disable the `{name}` HTTP Event Collector token.

See also

- data/inputs/http
- data/inputs/http/{name}
- data/inputs/http/{name}/enable
- collector/event

POST

Disable the `{name}` HTTP Event Collector token.

Request parameters

None

Returned values

Name	Description
_rcvbuf	Socket receive buffer size (bytes).
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	Host from which the indexer gets data.
index	Index to store generated events.

Name	Description
source	Default source for events with this token.
sourcetype	Default sourcetype for events with this token.
token	Token value for sending data to `collector/event` endpoint.

Example request and response

XML Request

```
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%3A%252F%252Fmyapp/disable
```

XML Response

```
 <title>http</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
 <updated>2015-01-30T12:59:44-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
 <link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch elided ...
 <s:messages/>
 <entry>
   <title>http://myapp</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp</id>
   <updated>2015-01-30T12:59:44-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="list"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/enable" rel="enable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="_rcvbuf">1572864</s:key>
       <s:key name="disabled">1</s:key>
       ... eai:acl elided ...
       <s:key name="eai:appName">system</s:key>
       <s:key name="eai:userName">nobody</s:key>
       <s:key name="host">$decideOnStartup</s:key>
       <s:key name="index">default</s:key>
       <s:key name="recursive">false</s:key>
       <s:key name="token">AABD8B82-2810-4BE8-823F-FE6C15ECB46E</s:key>
     </s:dict>
   </content>
 </entry>
```

data/inputs/http/{name}/enable

`https://<host>:<mPort>/services/data/inputs/http/{name}/enable`

Enable the `{name}` HTTP Event Collector token.

> The POST request to this endpoint reloads the HTTP Event Collector server, including when the server is already enabled and running.

See also

- data/inputs/http
- data/inputs/http/{name}
- data/inputs/http/{name}/disable
- collector/event

POST

Enable the `{name}` HTTP Event Collector token.

The POST request reloads the HTTP Event Collector server, including when the server is already enabled and running.

Request parameters

None

Returned values

Name	Description
_rcvbuf	Socket receive buffer size (bytes).
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	Host from which the indexer gets data.
index	Index to store generated events.
source	Default source for events with this token.
sourcetype	Default sourcetype for events with this token.
token	Token value for sending data to `collector/event` endpoint.

Example request and response

XML Request

```
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%3A%252F%252Fmyapp/enable
```

XML Response

```
...
 <title>http</title>
 <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
 <updated>2015-01-30T12:56:38-08:00</updated>
 <generator build="250128" version="20150120"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
 <link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
 ... opensearch elided ...
 <s:messages/>
 <entry>
   <title>http://myapp</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp</id>
   <updated>2015-01-30T12:56:38-08:00</updated>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="list"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="_rcvbuf">1572864</s:key>
       <s:key name="disabled">0</s:key>
       ... eai:acl elided ...
       <s:key name="eai:appName">system</s:key>
       <s:key name="eai:userName">nobody</s:key>
       <s:key name="host">$decideOnStartup</s:key>
       <s:key name="index">default</s:key>
       <s:key name="recursive">false</s:key>
       <s:key name="token">AABD8B82-2810-4BE8-823F-FE6C15ECB46E</s:key>
     </s:dict>
   </content>
 </entry>
```

data/inputs/http/{name}/rotate

`https://<host>:<mPort>/services/data/inputs/http/{name}/rotate`

Regenerate the `{name}` token value.

POST

Regenerate the `{name}` token value.

Request parameters

None

Returned values

Name	Description
token	Regenerated token value.

Example request and response

XML Request

```
curl -u admin:changeme
https://localhost:8089/servicesNS/nobody/splunk_httpinput/data/inputs/http/my_app_name/rotate -X post
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
        . . . . . .
        <s:key name="token">64D47EC6-C510-4519-A520-EC4CAA157B97</s:key>
        . . . . . .
</feed>
```

data/inputs/monitor

```
https://<host>:<mPort>/services/data/inputs/monitor
```

Access monitor inputs.

GET

List enabled and disabled monitor inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
_TCP_ROUTING	List of TCP forwarding groups, as specified in `outputs.conf`.
disabled	Indicates if inputs monitoring is disabled.
filecount	Number of files monitored.
host	Name of the Splunk host for which inputs are monitored.
index	The index in which to store the gathered data.
sourcetype	Source type being monitored. The source type of an event is the format of the data input from which it originates, such as access_combined or cisco_syslog. The source type determines how Splunk software formats your data.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/monitor
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/services/data/inputs/monitor</id>
  <updated>2011-07-10T14:25:53-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/monitor/_new" rel="create"/>
  <link href="/services/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>$SPLUNK_HOME/etc/splunk.version</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK
_HOME%252Fetc%252Fsplunk.version</id>
    <updated>2011-07-10T14:25:53-07:00</updated>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version"
rel="list"/>
    <link
href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version"
rel="edit"/>
    <link
href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_TCP_ROUTING">*</s:key>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="filecount">1</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">_internal</s:key>
        <s:key name="sourcetype">splunk_version</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new file or directory monitor input.

Request parameters

Name	Datatype	Description
blacklist	String	Specify a regular expression for a file path. The file path that matches this regular expression is not indexed.
check-index	Boolean	If set to true, the *index* value is checked to ensure that it is the name of a valid index.
check-path	Boolean	If set to true, the *name* value is checked to ensure that it exists.
crc-salt	String	A string that modifies the file tracking identity for files in this input. The magic value "<SOURCE>" invokes special behavior (see admin documentation).
disabled	Boolean	Indicates if input monitoring is disabled.
followTail	Boolean	If set to true, files that are seen for the first time is read from the end.
host	String	The value to populate in the host field for events from this data input.
host_regex	String	Specify a regular expression for a file path. If the path for a file matches this regular expression, the captured value is used to populate the host field for events from this data input. The regular expression must have one capture group.
host_segment	Number	Use the specified slash-separate segment of the filepath as the host field value.
ignore-older-than	String	Specify a time value. If the modification time of a file being monitored falls outside of this rolling time window, the file is no longer being monitored.
index	String	Which index events from this input should be stored in. Defaults to `default`.
name	String	**Required**. The file or directory path to monitor on the system.
recursive	Boolean	Setting this to `false` prevents monitoring of any subdirectories encountered within this data input.
rename-source	String	The value to populate in the source field for events from this data input. The same source should not be used for multiple data inputs.
sourcetype	String	The value to populate in the sourcetype field for incoming events.
time-before-close	Number	When Splunk software reaches the end of a file that is being read, the file is kept open for a minimum of the number of seconds specified in this value. After this period has elapsed, the file is checked again for more data.
whitelist	String	Specify a regular expression for a file path. Only file paths that match this regular expression are indexed.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor -d name=/var/log
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:27:57-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/monitor/{name}

`https://<host>:<mPort>/services/data/inputs/monitor/{name}`

Manage the `{name}` monitor input.

DELETE

Disable the named monitor data input and remove it from the configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:35:35-07:00</updated>
  <generator version="102807"/>
  <author>
```

```
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

List the properties of a single monitor data input.

Request parameters

None

Returned values

Name	Description
disabled	Indicates if inputs monitoring is disabled.
filecount	Number of files being monitored.
host	Name of the Splunk host for which inputs are monitored.
index	The index events from this input should be stored in.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:33:54-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/var/log</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog</id>
    <updated>2011-07-10T14:33:54-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog/members" rel="members"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>blacklist</s:item>
                <s:item>check-index</s:item>
                <s:item>check-path</s:item>
                <s:item>crc-salt</s:item>
                <s:item>followTail</s:item>
                <s:item>host</s:item>
                <s:item>host_regex</s:item>
                <s:item>host_segment</s:item>
                <s:item>ignore-older-than</s:item>
                <s:item>index</s:item>
                <s:item>recursive</s:item>
                <s:item>rename-source</s:item>
                <s:item>sourcetype</s:item>
                <s:item>time-before-close</s:item>
                <s:item>whitelist</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="filecount">108</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update properties of the named monitor input.

Request parameters

Name	Datatype	Description
blacklist	String	Specify a regular expression for a file path. The file path that matches this regular expression is not indexed.
check-index	Boolean	If set to true, the "index" value is checked to ensure that it is the name of a valid index.
check-path	Boolean	If set to true, the "name" value is checked to ensure that it exists.
crc-salt	String	A string that modifies the file tracking identity for files in this input. The magic value "<SOURCE>" invokes special behavior (see admin documentation).
disabled	Boolean	Indicates if input monitoring is disabled.
followTail	Boolean	If set to true, files that are seen for the first time is read from the end.
host	String	The value to populate in the host field for events from this data input.
host_regex	String	Specify a regular expression for a file path. If the path for a file matches this regular expression, the captured value is used to populate the host field for events from this data input. The regular expression must have one capture group.
host_segment	Number	Use the specified slash-separate segment of the filepath as the host field value.
ignore-older-than	String	Specify a time value. If the modification time of a file being monitored falls outside of this rolling time window, the file is no longer being monitored.
index	String	Which index events from this input should be stored in. Defaults to `default`.
recursive	Boolean	Setting this to "false" prevents monitoring of any subdirectories encountered within this data input.
rename-source	String	The value to populate in the source field for events from this data input. The same source should not be used for multiple data inputs.
sourcetype	String	The value to populate in the sourcetype field for incoming events.
time-before-close	Number	When Splunk software reaches the end of a file that is being read, the file is kept open for a minimum of the number of seconds specified in this value. After this period has elapsed, the file is checked again for more data.
whitelist	String	Specify a regular expression for a file path. Only file paths that match this regular expression are indexed.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog -d
recursive=false
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:35:28-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/monitor/{name}/members

`https://<host>:<mPort>/services/data/inputs/monitor/{name}/members`

List `{name}` monitor input files.

GET

List all files monitored under the named monitor input.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

The response includes a list of monitored files. See the following example for more details.

Example request and response

XML Request

```
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog/members
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:34:28-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
```

```
    <title>/var/log/acpid</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid</id>
    <updated>2011-07-10T14:34:28-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
  . . . elided . . .
</feed>
```

data/inputs/oneshot

`https://<host>:<mPort>/services/data/inputs/oneshot`

Access oneshot inputs in progress or queue a file for immediate indexing.

GET

Access oneshot inputs in progress.

Request parameters

None

Returned values

Name	Description
Bytes Indexed	Total number of bytes read and sent to the pipeline for indexing during a oneshot input. This total includes the uncompressed byte count from a source file that is compressed on disk.
Offset	Current position in the source file, indicating how much of the file is read. For compressed source files, this offset represents the position in the compressed format. You can obtain the percentage of a source file read by calculating offset/size.
Size	Size of the source file, in bytes. You can obtain the percentage of a source file read by calculating offset/size.
Sources Indexed	Indicates the number of sources read from a file in a compressed format such as tar or zip. A value of 0 indicates the source file was not compressed.
Spool Time	Time that the request was made to read the source file.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/oneshot
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>oneshotinput</title>
  <id>https://localhost:8089/services/data/inputs/oneshot</id>
  <updated>2011-07-08T01:48:04-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/oneshot/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/var/log/distccd.log</title>
    <id>https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fdistccd.log</id>
    <updated>2011-07-08T01:48:04-07:00</updated>
    <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fdistccd.log" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fdistccd.log" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Bytes Indexed">7200768</s:key>
        <s:key name="Offset">7200768</s:key>
        <s:key name="Size">449630160</s:key>
        <s:key name="Sources Indexed">0</s:key>
        <s:key name="Spool Time">Fri Jul  8 01:47:53 PDT 2011</s:key>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Queue a file for immediate indexing.

Usage details

The file being queued must be locally accessible from the server. This endpoint can handle any single file: plain, compressed or archive. The file is indexed in full, regardless of whether it is already indexed.

Request parameters

Name	Datatype	Default	Description
host	String		The value of the `host` field to be applied to data from this file.
host_regex	String		A regex to be used to extract a `host` field from the path. If the path matches this regular expression, the captured value is used to populate the host field for events from this data input. The regular expression must have one capture group.
host_segment	Number		Use the specified slash-separate segment of the path as the host field value.
index	String		The destination index for data processed from this file.
name	String		**Required**. The path to the file to be indexed. The file must be locally accessible by the server.
rename-source	String		The value of the `source` field to be applied to data from this file.
sourcetype	String		The value of the `sourcetype` field to be applied to data from this file.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/oneshot -d name=/var/log/messages
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>oneshotinput</title>
  <id>https://localhost:8089/services/data/inputs/oneshot</id>
  <updated>2011-07-08T01:48:04-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/oneshot/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/oneshot/{name}

`https://<host>:<mPort>/services/data/inputs/oneshot/{name}`

Get information about the `{name}` one-shot input.

GET

Access information about the `{name}` in-progress oneshot input.

Request parameters
None

Returned values

Name	Description
Bytes Indexed	Total number of bytes read and sent to the pipeline for indexing during a oneshot input. This total includes the uncompressed byte count from a source file that is compressed on disk.
Offset	Current position in the source file, indicating how much of the file is read. For compressed source files, this offset represents the position in the compressed format. You can obtain the percentage of a source file read by calculating offset/size.
Size	Size of the source file, in bytes. You can obtain the percentage of a source file read by calculating offset/size.
Sources Indexed	Indicates the number of sources read from a file in a compressed format such as tar or zip. A value of 0 indicates the source file was not compressed.
Spool Time	Time that the request was made to read the source file.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>oneshotinput</title>
  <id>https://localhost:8089/services/data/inputs/oneshot</id>
  <updated>2011-07-08T01:49:20-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/oneshot/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/var/log/messages</title>
    <id>https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages</id>
    <updated>2011-07-08T01:49:20-07:00</updated>
    <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Bytes Indexed">114822</s:key>
        <s:key name="Offset">114822</s:key>
        <s:key name="Size">114822</s:key>
        <s:key name="Sources Indexed">0</s:key>
        <s:key name="Spool Time">Fri Jul  8 01:48:04 PDT 2011</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/registry

`https://<host>:<mPort>/services/data/inputs/registry`
Access the Windows registry monitoring input.

GET

Get current registry monitoring configuration details.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
baseline	Indicates whether or not Splunk software should get a baseline of Registry events when it starts. Defaults to false. If true, the input captures a baseline for the specified hive when the input starts for the first time.
disabled	Indicats whether this input is disabled.
hive	Regular expression for Registry hives that this input should monitor for Registry access.

Name	Description
	Matches against the Registry key which was accessed. Events that contain hives that do not match the regular expression get filtered out. Events that contain hives that match the regular expression pass through.
index	Specifies the index that this input should send the data to. If no value is present, defaults to the default index.
monitorSubnodes	Indicates whether to monitor all Registry hives beneath the specified hive.
proc	Regular expression for processes this input should monitor for Registry access. It matches against the process name which performed the Registry access. Events generated by processes that do not match the regular expression get filtered out. Events generated by processes that match the regular expression pass through.
type	A regular expression that specifies the types of Registry events to monitor.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/registry
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/services/data/inputs/registry</id>
  <updated>2011-07-29T19:31:32-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/registry/_new" rel="create"/>
  <link href="/services/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Machine keys</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry/Machine%20keys</id>
    <updated>2011-07-29T19:31:32-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys/enable" rel="enable"/>
    <content type="text/xml">
```

```
      <s:dict>
        <s:key name="baseline">0</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="hive">HKLM</s:key>
        <s:key name="index">default</s:key>
        <s:key name="monitorSubnodes">1</s:key>
        <s:key name="proc">c:\.*</s:key>
        <s:key name="type">
          <s:list>
            <s:item>set</s:item>
            <s:item>create</s:item>
            <s:item>delete</s:item>
            <s:item>rename</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Creates new or modify existing registry monitoring settings.

Request parameters

Name	Datatype	Default	Description
baseline	Boolean		**Required**. Indicate whether to establish a baseline value for the registry keys. Use `1` to establish the baseline, `0` for no baseline.
hive	String		**Required**. Specify the registry hive for monitoring changes.
name	String		**Required**. Name of the configuration stanza.
proc	String		**Required**. Specify a regex for collecting changes if a process name matches the regex.
type	String		**Required**. List registry event types that you want to monitor. Separate each type with a pipe ('|') character. For example, `set | create | delete | rename`
disabled	Boolean		Indicates whether the monitoring is disabled.
index	String	default	The index in which to store the gathered data.
monitorSubnodes	Boolean	True	Indicates whether to monitor all registry hives beneath the specified hive.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/registry -d baseline=1 -d
```

```
hive="HKU\\.*" -d name=mykeys -d proc="c:\\.*" -d type="set|create|delete|rename"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:29:18-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/registry/{name}

`https://<host>:<mPort>/services/data/inputs/registry/{name}`

Manage registry monitoring `{name}` stanza.

DELETE

Delete a registry monitoring configuration stanza.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
```

```
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:36:54-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Gets current registry monitoring configuration stanza

Request parameters
None

Returned values

Name	Description
baseline	Indicates whether to get a baseline of Registry events when Splunk software starts.
disabled	Indicates if the input is disabled.
hive	Regular expression for Registry hives that this input should monitor for Registry access. Matches against the Registry key which was accessed. Events that contain hives that do not match the regular expression get filtered out. Events that contain hives that match the regular expression pass through.
index	Specifies the index that this input should send the data to. If no value is present, defaults to the default index.
monitorSubnodes	Indicates whether to monitor all Registry hives beneath the specified hive.
proc	Regular expression for processes this input should monitor for Registry access. It matches against the process name which performed the Registry access. Events generated by processes that do not match the regular expression get filtered out. Events generated by processes that match the regular expression pass through.
type	Regular expression that specifies the types of Registry events to monitor.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:33:21-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>mykeys</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry/mykeys</id>
    <updated>2011-07-29T19:33:21-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="baseline">1</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>disabled</s:item>
                <s:item>index</s:item>
                <s:item>monitorSubnodes</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>baseline</s:item>
                <s:item>hive</s:item>
                <s:item>proc</s:item>
                <s:item>type</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="hive">HKU</s:key>
        <s:key name="index">default</s:key>
        <s:key name="monitorSubnodes">1</s:key>
        <s:key name="proc">c:\.*</s:key>
        <s:key name="type">
```

```
          <s:list>
            <s:item>set</s:item>
            <s:item>create</s:item>
            <s:item>delete</s:item>
            <s:item>rename</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Modify the named registry monitoring stanza.

Request parameters

Name	Datatype	Default	Description
baseline	Number		**Required**. Specifies whether or not to establish a baseline value for the registry keys. 1 means yes, 0 no.
hive	String		**Required**. Specifies the registry hive under which to monitor for changes.
proc	String		**Required**. Specifies a regex. If specified, collect changes if a process name matches that regex.
type	String		**Required**. A list of registry events types that you want to monitor. Separate each type with a pipe ('|') character. For example: `set | create | delete | rename`
disabled	Number		Indicates whether the monitoring is disabled.
index	String	default	The index in which to store the gathered data.
monitorSubnodes	Boolean	True	Indicates whether to monitor all Registry hives beneath the specified hive.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys -d baseline=1
-d hive="HKU\\.*" -d proc="c:\\.*" -d type="set|create"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:36:07-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/script

`https://<host>:<mPort>/services/data/inputs/script`

Access scripted inputs.

GET

Get the configuration settings for scripted inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
disabled	Specifies whether the input script is disabled.
endtime	If available, the time when the script stopped executing.
group	The name of the inputstatus group, which is always "exec commands."
host	Host with which these data are identified.
index	Sets the index for events from this input. Defaults to the main index.
interval	An integer or cron schedule. Specifies how often to execute the specified script, in seconds or a valid cron schedule. For a cron schedule, the script is not executed on start-up.
source	The source key/field for events from this input. Defaults to the input file path. Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'.
sourcetype	

Name	Description
	Sets the sourcetype key/field for events from this input. If unset, Splunk software picks a source type based on various aspects of the data. There is no hard-coded default. For more information, see the documentation for the sourcetype parameter for the POST operation.
starttime	If available, the time the when the script was executed.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/script
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/services/data/inputs/script</id>
  <updated>2011-07-09T20:16:11-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/script/_new" rel="create"/>
  <link href="/services/data/inputs/script/_reload" rel="_reload"/>
  <link href="/services/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/Applications/splunk4.3/etc/apps/unix/bin/cpu.sh</title>
    <id>https://localhost:8089/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh</id>
    <updated>2011-07-09T20:16:11-07:00</updated>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh" rel="list"/>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh" rel="edit"/>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="endtime">Sat Jul  9 20:15:54 2011</s:key>
        <s:key name="group">exec commands</s:key>
        <s:key name="host">myhost.splunk.com</s:key>
        <s:key name="index">os</s:key>
        <s:key name="interval">30</s:key>
        <s:key name="source">cpu</s:key>
        <s:key name="sourcetype">cpu</s:key>
        <s:key name="starttime">Sat Jul  9 20:15:52 2011</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Configure scripted input settings.

Request parameters

Name	Datatype	Default	Description
disabled	Boolean		Specifies whether the input script is disabled.
host	String		Sets the host for events from this input. Defaults to whatever host sent the event.
index	String	default	Sets the index for events from this input. Defaults to the main index.
interval	Number	60.0	**Required**. Specify an integer or cron schedule. This parameter specifies how often to execute the specified script, in seconds or a valid cron schedule. If you specify a cron schedule, the script is not executed on start-up.
name	String		**Required**. Specify the name of the scripted input.
passAuth	String		User to run the script as. If you provide a username, Splunk software generates an auth token for that user and passes it to the script.
rename-source	String		Specify a new name for the source field for the script.
source	String		Sets the source key/field for events from this input. Defaults to the input file path. Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'. **Note:** Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.
sourcetype	String		Sets the sourcetype key/field for events from this input. If unset, Splunk software picks a source type based on various aspects of the data. As a convenience, the chosen string is prepended with 'sourcetype::'. There is no hard-coded default. Sets the sourcetype key initial value. The key is used during parsing/indexing, in particular to set the source type field during indexing. It is also the source type field used at search time. Primarily used to explicitly declare the source type for this data, as opposed to allowing it to be determined using automated methods. This is typically important both for searchability and for applying the relevant configuration for this type of data during parsing and indexing.

Name	Datatype	Default	Description

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script -d
name=/Applications/splunk4.3/etc/apps/myApp/bin/myScript.sh -d disabled=true -d interval=3600
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
  <updated>2011-07-09T20:25:17-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/script/restart

`https://<host>:<mPort>/services/data/inputs/script/restart`

Allows for restarting scripted inputs.

POST

Causes a restart on a given scripted input.

Request parameters

Name	Datatype	Default	Description
script	String		**Required**. Path to the script to be restarted. This path must match an already-configured existing scripted input.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script/restart -d
script=/Applications/splunk/bin/scripts/myScript.sh
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
  <updated>2011-07-09T20:38:38-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/script/{name}

`https://<host>:<mPort>/services/data/inputs/script/{name}`

Manage the `{name}` scripted input.

DELETE

Removes the `{name}` scripted input.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/script
```

```
/%252FApplications%252Fsplunk4.3%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
  <updated>2011-07-09T20:29:18-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Returns the configuration settings for the `{name}` scripted input.

Request parameters

None

Returned values

Name	Description
disabled	Specifies whether the input script is disabled.
group	The name of the inputstatus group, which is always "exec commands."
host	Host these data are identified with.
index	Sets the index for events from this input. Defaults to the main index.
interval	An integer or cron schedule. Specifies how often to execute the specified script, in seconds or a valid cron schedule. For a cron schedule, the script is not executed on start-up.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
  <updated>2011-07-09T21:53:43-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/Applications/splunk/etc/apps/myApp/bin/myScript.sh</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh</id>
    <updated>2011-07-09T21:53:43-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>disabled</s:item>
                <s:item>host</s:item>
                <s:item>index</s:item>
                <s:item>interval</s:item>
                <s:item>rename-source</s:item>
                <s:item>source</s:item>
                <s:item>sourcetype</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="group">exec commands</s:key>
        <s:key name="host">ombroso-mbp15.splunk.com</s:key>
        <s:key name="index">default</s:key>
        <s:key name="interval">3600</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Configures settings for the `{name}` scripted input.

Request parameters

Name	Datatype	Default	Description
disabled	Boolean		Specifies whether the input script is disabled.
host	String		Sets the host for events from this input. Defaults to whatever host sent the event.
index	String	default	Sets the index for events from this input. Defaults to the main index.
interval	Number	60.0	Specify an integer or cron schedule. This parameter specifies how often to execute the specified script, in seconds or a valid cron schedule. If you specify a cron schedule, the script is not executed on start-up.
passAuth	String		User to run the script as. If you provide a username, Splunk software generates an auth token for that user and passes it to the script.
rename-source	String		Specify a new name for the source field for the script.
source	String		Sets the source key/field for events from this input. Defaults to the input file path. Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'. **Note:** Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieived. Consider use of source types, tagging, and search wildcards before overriding this value.
sourcetype	String		Sets the sourcetype key/field for events from this input. If unset, Splunk software picks a source type based on various aspects of the data. As a convenience, the chosen string is prepended with 'sourcetype::'. There is no hard-coded default. Sets the sourcetype key initial value. The key is used during parsing/indexing, in particular to set the source type field during indexing. It is also the source type field used at search time.

Name	Datatype	Default	Description
			Primarily used to explicitly declare the source type for this data, as opposed to allowing it to be determined using automated methods. This is typically important both for searchability and for applying the relevant configuration for this type of data during parsing and indexing.

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script
/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh -d interval=86400
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
  <updated>2011-07-09T20:27:59-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/tcp/cooked

```
https://<host>:<mPort>/services/data/inputs/tcp/cooked
```

Access cooked TCP input information and create new containers for managing cooked data.

Usage details
Forwarders can transmit three types of data: raw, unparsed, or parsed. "Cooked" data refers to parsed and unparsed formats.

GET

Access information about all cooked TCP inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
_rcvbuf	[Deprecated]
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
group	Set to `listenerports` for listening ports.
host	The default value to fill in for events lacking a host value.
index	The index in which to store generated events.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/cooked
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/services/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:50:50-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>9993</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9993</id>
    <updated>2011-07-10T14:50:50-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="group">listenerports</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new container for managing cooked data.

Request parameters

Name	Datatype	Default	Description
SSL	Boolean		If SSL is not already configured, error is returned
connection_host	Enum	dns	Valid values: (ip | dns | none) Set the host for the remote server that is sending data. `ip` sets the host to the IP address of the remote server sending data. `dns` sets the host to the reverse DNS entry for the IP address of the remote server sending data. `none` leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is `dns`.
disabled	Boolean		Indicates whether the input is disabled.
host	String		The default value to fill in for events lacking a host value.
name	Number		**Required**. The port number of this input.
queue	"parsingQueue" | "indexQueue"	"parsingQueue"	Specifies where the input processor should deposit the events it reads.
restrictToHost	String		Restrict incoming connections on this port to the host specified here.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked -d name=9998
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:52:33-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/tcp/cooked/{name}

`https://<host>:<mPort>/services/data/inputs/tcp/cooked/{name}`

Manage cooked TCP inputs for the `{name}` host or port.

DELETE

Remove the cooked TCP inputs for `port` or `host:port` specified by `{name}`.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
```

```
https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/tiny:9998
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:54:45-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access information for the `{name}` cooked TCP input.

Usage details

If port is restricted to a host, `{name}` should be a URI-encoded `host:port`.

Request parameters

None

Returned values

Name	Description
_rcvbuf	[Deprecated]
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
group	Set to `listenerports` for listening ports.
host	The default value to fill in for events lacking a host value.
index	The index in which to store generated events.
restrictToHost	Restrict incoming connections on this port to the specified host.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:52:40-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>9998</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998</id>
    <updated>2011-07-10T14:52:40-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>SSL</s:item>
                <s:item>connection_host</s:item>
                <s:item>disabled</s:item>
                <s:item>host</s:item>
                <s:item>index</s:item>
                <s:item>queue</s:item>
                <s:item>restrictToHost</s:item>
                <s:item>source</s:item>
                <s:item>sourcetype</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="group">listenerports</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update the container for managing cooked data.

Request parameters

Name	Datatype	Default	Description
SSL	Boolean		If SSL is not already configured, error is returned
connection_host	Enum	ip	Valid values: (ip | dns | none) Set the host for the remote server that is sending data. `ip` sets the host to the IP address of the remote server sending data. `dns` sets the host to the reverse DNS entry for the IP address of the remote server sending data. `none` leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is `ip`.
disabled	Boolean		Indicates whether the input is disabled.
host	String		The default value to fill in for events lacking a host value.
restrictToHost	String		Restrict incoming connections on this port to the host specified here.

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998 -d
restrictToHost=tiny
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:52:54-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/tcp/cooked/{name}/connections

`https://<host>:<mPort>/services/data/inputs/tcp/cooked/{name}/connections`
Get active connections to the `{name}` port.

GET

List active connections to the `{name}` port.

Request parameters

None

Returned values

Name	Description
connection	Identifies the connection to port.
servername	Server name of forwarder connecting to this port.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/connections
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked</id>
  <updated>2011-07-13T14:55:18-0700</updated>
  <generator version="101277"/>
  <author>
```

```
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Cooked:9998:127.0.0.1:20089</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked
/Cooked%3A9998%3A127.0.0.1%3A20089</id>
    <updated>2011-07-13T14:55:18-0700</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089"
rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089"
rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="connection">9998:127.0.0.1:20089</s:key>
        ... eai:acl node elided ...
        <s:key name="servername">fool03.splunk.com</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/tcp/raw

`https://<host>:<mPort>/services/data/inputs/tcp/raw`

Container for managing raw tcp inputs from forwarders.

Forwarders can transmit three types of data: raw, unparsed, or parsed. Cooked data refers to parsed and unparsed formats.

Authentication and authorization

The `edit_tcp` capability is required for this endpoint.

GET

Get information about all raw TCP inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
_rcvbuf	[Deprecated]
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
group	Set to `listenerports` for listening ports.
host	Host from which the indexer gets data.
index	The index in which to store generated events.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/raw
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/services/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:30-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>44000</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44000</id>
    <updated>2011-07-08T02:30:30-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="group">listenerports</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new data input for accepting raw TCP data.

Request parameters

Name	Datatype	Default	Description
connection_host	Enum	dns	Valid values: (ip | dns | none) Set the host for the remote server that is sending data. `ip` sets the host to the IP address of the remote server sending data. `dns` sets the host to the reverse DNS entry for the IP address of the remote server sending data. `none` leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is `ip`.
disabled	Boolean		Indicates whether the inputs are disabled.
host	String		Host from which the indexer gets data.
index	String	default	Index to store generated events.
name required	String		The input port which receives raw data.
queue	Enum		Valid values: (parsingQueue | indexQueue) Specifies where the input processor should deposit the events it reads. Defaults to parsingQueue. Set queue to `parsingQueue` to apply props.conf and other parsing rules to your data. For more information about props.conf and rules for timestamping and linebreaking, refer to `props.conf` and the online documentation at "Monitor files and directories with inputs.conf" Set queue to `indexQueue` to send your data directly into the index.

Name	Datatype	Default	Description
rawTcpDoneTimeout	Number		Specifies in seconds the timeout value for adding a Done-key. Default value is 10 seconds. If a connection over the port specified by `name` remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is completely received.
restrictToHost	String		Allows for restricting this input to only accept data from the host specified here.
SSL	Boolean		
source	String		Sets the source key/field for events from this input. Defaults to the input file path. Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'. *Note:* Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.
sourcetype	String		Set the source type for events from this input. "sourcetype=" is automatically prepended to <string>. Defaults to audittrail (if signedaudit=true) or fschange (if signedaudit=false).

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw -d name=44343
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:30-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/tcp/raw/{name}

`https://<host>:<mPort>/services/data/inputs/tcp/raw/{name}`

Manage raw inputs for the `{name}` host or port.

Authentication and authorization

The `edit_tcp` capability is additionally required for this endpoint.

DELETE

Remove the raw inputs for port or host:port specified by `{name}`

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:31-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Returns information about raw TCP input port {name}.

If port is restricted to a host, name should be URI-encoded host:port.

Request parameters

None

Returned values

Name	Description
_rcvbuf	[Deprecated]
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
group	Set to `listenerports` for listening ports.
host	Host from which the indexer gets data.
index	Index to store generated events.
restrictToHost	Restrict incoming connections on this port to the specified host.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:37:09-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>44343</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343</id>
    <updated>2011-07-08T02:37:09-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>SSL</s:item>
                <s:item>connection_host</s:item>
                <s:item>disabled</s:item>
                <s:item>host</s:item>
                <s:item>index</s:item>
                <s:item>queue</s:item>
                <s:item>restrictToHost</s:item>
                <s:item>source</s:item>
                <s:item>sourcetype</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="group">listenerports</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Updates the container for managing raw data.

Request parameters

Name	Datatype	Default	Description
SSL	Boolean		
connection_host	Enum	dns	Valid values: (ip | dns | none)

Name	Datatype	Default	Description
			Set the host for the remote server that is sending data. `ip` sets the host to the IP address of the remote server sending data. `dns` sets the host to the reverse DNS entry for the IP address of the remote server sending data. `none` leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is `ip`.
disabled	Boolean		Indicates whether the inputs are disabled.
host	String		Host from which the indexer gets data.
index	String	default	Index to store generated events.
queue	Enum		Valid values: (parsingQueue | indexQueue) Specifies where the input processor should deposit the events it reads. Defaults to parsingQueue. Set queue to `parsingQueue` to apply props.conf and other parsing rules to your data. For more information about props.conf and rules for timestamping and linebreaking, refer to `props.conf` and Monitor files and directories with inputs.conf. Set queue to `indexQueue` to send your data directly into the index.
rawTcpDoneTimeout	Number		Specifies in seconds the timeout value for adding a Done-key. Default value is 10 seconds. If a connection over the port specified by `name` remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is completely received.
restrictToHost	String		Allows for restricting this input to only accept data from the host specified here.
source	String		Sets the source key/field for events from this input. Defaults to the input file path. Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'. *Note:* Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.
sourcetype	String		Set the source type for events from this input. "sourcetype=" is automatically prepended to <string>.

Name	Datatype	Default	Description
			Defaults to audittrail (if signedaudit=true) or fschange (if signedaudit=false).

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343 -d
sourcetype=syslog
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:30-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/tcp/raw/{name}/connections

`https://<host>:<mPort>/services/data/inputs/tcp/raw/{name}/connections`
Get active connections the `{name}` host or port.

Authentication and authorization
The `edit_tcp` capability is additionally required for this endpoint.

GET

View all connections to the named data input.

Request parameters
None

Returned values

Name	Description
connection	IP address and port of the source connecting to this TCP input port.
servername	DNS name of the source connecting to this TCP input port.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/raw/9998/connections
```

XML Response

```
...
  <title>raw</title>
  <id>https://localhost:8089/services/data/inputs/tcp/raw</id>
  <updated>2011-07-13T16:14:33-07:00</updated>
  <generator version="103477"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Raw:9998:127.0.0.1</title>
    <id>https://localhost:8089/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1</id>
    <updated>2011-07-13T16:14:33-07:00</updated>
    <link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="list"/>
    <link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1/_reload" rel="_reload"/>
    <link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="edit"/>
    <link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="connection">9998:127.0.0.1</s:key>
        ... eai:acl node elided ...
        <s:key name="servername"></s:key>
      </s:dict>
    </content>
  </entry>
```

data/inputs/tcp/splunktcptoken

`https://<host>:<mPort>/services/data/inputs/tcp/splunktcptoken`
Manage receiver access using tokens.

Usage details
Get information on all receiver tokens or create a new token. To edit or delete an existing token, see data/inputs/tcp/splunktcptoken/{name}.

Note: Configure the forwarder with the same token as the receiver to ensure that the forwarder receives data.

Authentication and Authorization:
The `edit_splunktcp_token` capability is required for this endpoint.

GET

Return all configured tokens.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Response data keys are returned for each receiver token.

Name	Description
host	Host from which the indexer gets data.
index	Index to store generated events.
token	Token value.

Example request and response

XML Request

```
curl  -k -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken
```

XML Response

```
<title>splunktcptoken</title>
  <id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
  <updated>2015-09-16T09:31:52-07:00</updated>
  <generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/splunktcptoken/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_reload" rel="_reload"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_acl" rel="_acl"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>splunktcptoken://tok1</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken
/splunktcptoken%3A%252F%252Ftok1</id>
    <updated>2015-09-16T09:31:52-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="list"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="remove"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="host">$decideOnStartup</s:key>
        <s:key name="index">default</s:key>
        <s:key name="token">99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>splunktcptoken://tok3</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken
/splunktcptoken%3A%252F%252Ftok3</id>
    <updated>2015-09-16T09:31:52-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok3"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok3"
rel="list"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok3/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok3"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok3"
rel="remove"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok3/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="host">$decideOnStartup</s:key>
        <s:key name="index">default</s:key>
        <s:key name="token">4EFFBD13-B26F-4F3A-BED9-03850001EDA1</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create a new token.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Datatype	Default	Description
name	String	None	Required. Name for the token to create.
token	String	None	Optional. Token value to use. If unspecified, a token is generated automatically.

Returned values

Name	Description
host	Host from which the indexer gets data.
index	Index to store generated events.
token	Token value.

Example request and response

XML Request

```
curl  -k -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken -d "name=tok1" -d
"token=99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF"
```

XML Response

```
 <title>splunktcptoken</title>
  <id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
  <updated>2015-09-16T09:27:03-07:00</updated>
  <generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/splunktcptoken/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_reload" rel="_reload"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>splunktcptoken://tok1</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken
/splunktcptoken%3A%252F%252Ftok1</id>
    <updated>2015-09-16T09:27:03-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="list"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="remove"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="host">$decideOnStartup</s:key>
        <s:key name="index">default</s:key>
        <s:key name="token">99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF</s:key>
      </s:dict>
    </content>
  </entry>
```

data/inputs/tcp/splunktcptoken/{name}

`https://<host>:<mPort>/services/data/inputs/tcp/splunktcptoken/{name}`
Manage existing receiver tokens.

Authentication and Authorization

The `edit_splunktcp_token` capability is required for this endpoint.

GET

Access token information.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
host	Host from which the indexer gets data.
index	Index to store generated events.
token	Token value.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/splunktcptoken
```

XML Response

```
...
 <title>splunktcptoken</title>
  <id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
  <updated>2015-09-16T09:28:22-07:00</updated>
  <generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/splunktcptoken/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_reload" rel="_reload"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>splunktcptoken://tok1</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken
/splunktcptoken%3A%252F%252Ftok1</id>
    <updated>2015-09-16T09:28:22-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="list"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="remove"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
```

```
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>disabled</s:item>
                <s:item>token</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>.*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="host">$decideOnStartup</s:key>
        <s:key name="index">default</s:key>
        <s:key name="token">99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update the `{name}` token.

Request parameters

Name	Datatype	Default	Description
token	String	None	New token value.

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
host	Host from which the indexer gets data.
index	Index to store generated events.
token	Token value.

Example request and response

XML Request

```
curl  -k -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken/tok1
```

XML Response

```
...
    <title>splunktcptoken://tok1</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken
/splunktcptoken%3A%252F%252Ftok1</id>
    <updated>2015-09-16T09:28:22-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="list"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1"
rel="remove"/>
    <link
href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
```

```
              <s:list>
                <s:item>disabled</s:item>
                <s:item>token</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>.*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="host">$decideOnStartup</s:key>
        <s:key name="index">default</s:key>
        <s:key name="token">99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF</s:key>
...
```

DELETE

Delete the `{name}` token.

Request parameters

None.

Returned values

Name	Description
host	Host from which the indexer gets data.
index	Index to store generated events.
token	Token value.

Example request and response

XML Request

```
curl -k -X "DELETE" -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken/tok1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>splunktcptoken</title>
  <id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
  <updated>2015-09-16T09:34:51-07:00</updated>
  <generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
  <author>
```

```
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/splunktcptoken/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_reload" rel="_reload"/>
  <link href="/services/data/inputs/tcp/splunktcptoken/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/inputs/tcp/ssl

`https://<host>:<mPort>/services/data/inputs/tcp/ssl`

Provides access to the SSL configuration of a Splunk server.

GET

Get SSL configuration details. There is only one SSL configuration for all input ports.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
_rcvbuf	[Deprecated]
cipherSuite	Specifies list of acceptable ciphers to use in ssl.
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	Host from which the indexer gets data.
index	Index to store generated events.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/ssl
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
```

```
  <title>ssl</title>
  <id>https://localhost:8089/services/data/inputs/tcp/ssl</id>
  <updated>2011-07-12T15:02:58-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/ssl/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title/>
    <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/tcp/ssl/</id>
    <updated>2011-07-12T15:02:58-07:00</updated>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/" rel="list"/>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl//_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="cipherSuite">ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="host">ombroso-mbp15.splunk.com</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/tcp/ssl/{name}

`https://<host>:<mPort>/services/data/inputs/tcp/ssl/{name}`

Access or update the SSL configuration for the `{name}` host.

GET

Returns the SSL configuration for the host `{name}`.

Request parameters
None

Returned values

Name	Description

Name	Description
_rcvbuf	[Deprecated]
cipherSuite	Specifies list of acceptable ciphers to use in ssl.
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
host	Host from which the indexer gets data.
index	Index to store generated events.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/ssl/ssl
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>ssl</title>
  <id>https://localhost:8089/services/data/inputs/tcp/ssl</id>
  <updated>2011-07-12T15:04:41-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/ssl/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title/>
    <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/tcp/ssl/</id>
    <updated>2011-07-12T15:04:41-07:00</updated>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/" rel="list"/>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl//_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="cipherSuite">ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="host">ombroso-mbp15.splunk.com</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Configure SSL for the `{name}` host.

Request parameters

Name	Datatype	Default	Description
disabled	Boolean		Indicates whether the inputs are disabled.
password	String		Server certificate password, if any.
requireClientCert	Boolean		Determines whether a client must authenticate.
rootCA	String		Certificate authority list (root file)
serverCert	String		Full path to the server certificate.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/ssl/ssl -d disabled=true
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>ssl</title>
  <id>https://localhost:8089/services/data/inputs/tcp/ssl</id>
  <updated>2011-07-12T15:05:42-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/ssl/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/udp

```
https://<host>:<mPort>/services/data/inputs/udp
```

Access or create UDP data inputs.

GET

List enabled and disabled UDP data inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
_rcvbuf	Socket receive buffer size (bytes).
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
group	Set to `listenerports` for listening ports.
host	Host from which the indexer gets data.
index	Index to store generated events.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/udp
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/services/data/inputs/udp</id>
  <updated>2011-07-08T14:11:57-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/udp/_new" rel="create"/>
  <link href="/services/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>44000</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44000</id>
    <updated>2011-07-08T14:11:57-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44000/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="group">listenerports</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new UDP data input.

Request parameters

Name	Datatype	Default	Description
connection_host	Enum	ip	Valid values: (ip | dns | none) Set the host for the remote server that is sending data. `ip` sets the host to the IP address of the remote server sending data. `dns` sets the host to the reverse DNS entry for the IP address of the remote server sending data. `none` leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is `ip`.
disabled	Boolean		Indicates if the input is disabled.
host	String		The value to populate in the host field for incoming events. This is used during parsing/indexing, in particular to set the host field. It is also the host field used at search time.
index	String	default	Which index events from this input should be stored in.

Name	Datatype	Default	Description
name	String		**Required**. The UDP port that this input should listen on.
no_appending_timestamp	Boolean		If set to true, prevents Splunk software from prepending a timestamp and hostname to incoming events.
no_priority_stripping	Boolean		If set to true, Splunk software does not remove the priority field from incoming syslog events.
queue	String		Which queue events from this input should be sent to. Generally this does not need to be changed.
restrictToHost	String		Restrict incoming connections on this port to the host specified here. If this is not set, the value specified in `[udp://<remote server>:<port>]` in `inputs.conf` is used.
source	String		The value to populate in the source field for incoming events. The same source should not be used for multiple data inputs.
sourcetype	String		The value to populate in the sourcetype field for incoming events.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp -d name=44321
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:13-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/udp/{name}

```
https://<host>:<mPort>/services/data/inputs/udp/{name}
```

Manage the `{name}` UDP host or port.

DELETE

Disable the named UDP data input and remove it from the configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:53-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

List the properties of a single UDP data input port or `host:port {name}`.

Usage details
If port is restricted to a host, `{name}` should be URI-encoded `host:port`.

Request parameters
None

Returned values

Name	Description
_rcvbuf	Socket receive buffer size (bytes).
disabled	Input disabled indicator: `0` = Input Not disabled, `1` = Input disabled.
group	Set to `listenerports` for listening ports.
host	Host from which the indexer gets data.
index	Index to store generated events.

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:27-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>44321</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321</id>
    <updated>2011-07-08T14:12:27-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>connection_host</s:item>
                <s:item>host</s:item>
                <s:item>index</s:item>
                <s:item>no_appending_timestamp</s:item>
                <s:item>no_priority_stripping</s:item>
                <s:item>queue</s:item>
                <s:item>source</s:item>
                <s:item>sourcetype</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="group">listenerports</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">default</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Edit properties of the named UDP data input.

Request parameters

Name	Datatype	Default	Description
connection_host	Enum	ip	Valid values: (ip | dns | none) Set the host for the remote server that is sending data. `ip` sets the host to the IP address of the remote server sending data. `dns` sets the host to the reverse DNS entry for the IP address of the remote server sending data. `none` leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is `ip`.
disabled	Boolean		Indicates if the input is disabled.
host	String		The value to populate in the host field for incoming events. This is used during parsing/indexing, in particular to set the host field. It is also the host field used at search time.
index	String	default	Which index events from this input should be stored in.

Name	Datatype	Default	Description
no_appending_timestamp	Boolean		If set to true, prevents Splunk software from prepending a timestamp and hostname to incoming events.
no_priority_stripping	Boolean		If set to true, Splunk software does not remove the priority field from incoming syslog events.
queue	String		Which queue events from this input should be sent to. Generally this does not need to be changed.
restrictToHost	String		Restrict incoming connections on this port to the host specified here. If this is not set, the value specified in [udp://<remote server>:<port>] in inputs.conf is used.
source	String		The value to populate in the source field for incoming events. The same source should not be used for multiple data inputs.
sourcetype	String		The value to populate in the sourcetype field for incoming events.

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321 -d
sourcetype=syslog
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:47-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/udp/{name}/connections

`https://<host>:<mPort>/services/data/inputs/udp/{name}/connections`

List connections to the `{name}` host or port.

GET

List connections to the `{name}` host or port.

Request parameters
None

Returned values

Name	Description
disabled	Indicates whether the inputs are disabled.
group	Set to 'listenerports' for listening ports.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/9998/connections
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-13T17:08:18-07:00</updated>
  <generator version="103477"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>127.0.0.1</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/127.0.0.1</id>
    <updated>2011-07-13T17:08:18-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="group">hosts</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/win-event-log-collections

```
https://<host>:<mPort>/services/data/inputs/win-event-log-collections
```

Provides access to all configured event log collections.

GET

Retrieve a list of configured event log collections.

Request parameters

Name	Datatype	Default	Description
lookup_host	String		For internal use. Used by the UI when editing the initial host from which we gather event log data.

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
disabled	Indicates if the input is disabled.
hosts	Hosts you are monitoring.
index	Index to store data. If not specified defaults to the default index.
logs	List of event log channels to monitor.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/win-event-log-collections
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/services/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T11:26:47-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/services/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>localhost</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost<
/id>
    <updated>2011-07-27T11:26:47-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="edit"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/enable"
rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="hosts">localhost</s:key>
        <s:key name="index">default</s:key>
        <s:key name="logs">
          <s:list>
            <s:item>Application</s:item>
            <s:item>ForwardedEvents</s:item>
            <s:item>HardwareEvents</s:item>
            <s:item>Internet Explorer</s:item>
            <s:item>Security</s:item>
            <s:item>Setup</s:item>
            <s:item>System</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create or modify existing event log collection settings.

Usage details

You can configure both native and WMI collections with this endpoint.

Request parameters

Name	Datatype	Default	Description
hosts	String		A comma-separated list of additional hosts to be used for monitoring. The first host should be specified with "lookup_host", and the additional ones using this parameter.
index	String	default	The index in which to store the gathered data.
logs	String		List of event log names from which to gather data: • WMI collection format (CSV) example: `logs=Application%2CSystem%2CSetup%2CSecurity` • Native event log collection format example: `logs=Application&logs=System&logs=Setup`
lookup_host	String		**Required**. Host from which to monitor log events. To specify additional hosts to be monitored using WMI, use the "hosts" parameter.
name	String		**Required**. Collection name. This name appears in configuration file, as well as the source and the sourcetype of the indexed data. If the value is "localhost", it uses native event log collection; otherwise, it uses WMI.

Returned values

Name	Description
disabled	Indicates if the input is disabled.
hosts	Monitored hosts.
index	Index to store data.
logs	List of event log channels to monitor.
lookup_host	Host from which to monitor log events.
name	The name of the collection. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is "localhost", it uses native event log collection; otherwise, it uses WMI

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections -d
lookup_host=localhost -d name=mylogs -d logs=Application,System
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T11:56:24-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>localhost</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost<
/id>
    <updated>2011-07-27T11:56:24-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="hosts">localhost</s:key>
        <s:key name="index">default</s:key>
        <s:key name="logs">
          <s:list>
            <s:item>Application</s:item>
            <s:item>ForwardedEvents</s:item>
            <s:item>HardwareEvents</s:item>
            <s:item>Internet Explorer</s:item>
            <s:item>Security</s:item>
            <s:item>Setup</s:item>
            <s:item>System</s:item>
          </s:list>
        </s:key>
        <s:key name="lookup_host">localhost</s:key>
        <s:key name="name">localhost</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/win-event-log-collections/{name}

`https://<host>:<mPort>/services/data/inputs/win-event-log-collections/{name}`

Manage the `{name}` Windows event log.

DELETE

Deletes an event log collection.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T13:45:24-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Gets event log collection configurations.

Request parameters

Name	Datatype	Default	Description
lookup_host	String		For internal use. Used by the UI when editing the initial host from which we gather event log data.

Returned values

Name	Description
disabled	Indicates if the input is disabled.
hosts	Monitored hosts.
index	Index to store data. If not specified defaults to the default index.
logs	List of event log channels to monitor.
lookup_host	Host from which to monitor log events.
name	The name of the collection. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.

Example request and response

XML Request

```
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T12:00:38-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>mylogs</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs</id>
    <updated>2011-07-27T12:00:38-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/disable"
```

```
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>hosts</s:item>
                <s:item>index</s:item>
                <s:item>logs</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>lookup_host</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="hosts"/>
        <s:key name="index">default</s:key>
        <s:key name="logs">
          <s:list>
            <s:item>Application,System</s:item>
          </s:list>
        </s:key>
        <s:key name="lookup_host">localhost</s:key>
        <s:key name="name">mylogs</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Modify an existing event log collection.

Request parameters

Name	Datatype	Default	Description
hosts	String		A comma-separated list of additional hosts to be used for monitoring. The first host should be specified with "lookup_host", and the additional ones using this parameter.
index	String	default	The index in which to store the gathered data.
logs	String		A comma-separated list of event log names to gather data from.
lookup_host	String		**Required**. This is a host from which we monitor log events. To specify additional hosts to be monitored using WMI, use the "hosts" parameter.

Name	Datatype	Default	Description

Returned values

Name	Description
disabled	Indicates if the input is disabled.
hosts	Monitored hosts.
index	Index to store data.
logs	List of event log channels to monitor.
lookup_host	Host from which to monitor log events.
name	The name of the collection. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.

Example request and response

XML Request

```
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs -d
lookup_host=localhost -d logs=Application
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T13:43:46-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>localhost</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost<
/id>
    <updated>2011-07-27T13:43:46-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="edit"/>
    <content type="text/xml">
```

```
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="hosts">localhost</s:key>
        <s:key name="index">default</s:key>
        <s:key name="logs">
          <s:list>
            <s:item>Application</s:item>
            <s:item>ForwardedEvents</s:item>
            <s:item>HardwareEvents</s:item>
            <s:item>Internet Explorer</s:item>
            <s:item>Security</s:item>
            <s:item>Setup</s:item>
            <s:item>System</s:item>
          </s:list>
        </s:key>
        <s:key name="lookup_host">localhost</s:key>
        <s:key name="name">localhost</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/win-wmi-collections

`https://<host>:<mPort>/services/data/inputs/win-wmi-collections`

Access configured WMI collections.

GET

Access configured WMI collections.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
class	The WMI performance object class being monitored.
disabled	Indicates whther the input is disbled.
fields	The WMI performance counters being monitored.
index	The index to which you are sending input data.
instances	Instances of the WMI performance counter.

Name	Description
interval	The interval, in seconds, at which the WMI provider(s) are queried.
name	the name of the input.
server	The server you are monitoring.
wql	The actual WQL query for monitoring the performance object.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/win-wmi-collections
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
  <id>https://10.1.5.157:8089/services/data/inputs/win-wmi-collections</id>
  <updated>2011-07-27T14:00:24-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/win-wmi-collections/_new" rel="create"/>
  <link href="/services/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>CPUTime</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime</id>
    <updated>2011-07-27T14:00:24-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="edit"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="class">Win32_PerfFormattedData_PerfOS_Processor</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="fields">
          <s:list>
            <s:item>PercentProcessorTime</s:item>
            <s:item>PercentUserTime</s:item>
          </s:list>
        </s:key>
        <s:key name="index">default</s:key>
        <s:key name="instances">
          <s:list>
            <s:item>_Total</s:item>
          </s:list>
        </s:key>
        <s:key name="interval">3</s:key>
        <s:key name="name"/>
        <s:key name="server">localhost</s:key>
        <s:key name="wql">SELECT PercentProcessorTime,PercentUserTime FROM
Win32_PerfFormattedData_PerfOS_Processor WHERE Name="_Total"</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create or modify existing WMI collection settings.

Request parameters

Name	Datatype	Default	Description
classes	String		**Required**. A valid WMI class name.
disabled	Number	`0`	Disables the given collection.
fields	String	`1. *`	Properties (fields) that you want to gather from the given class. Specify each property as a separate argument to the POST operation.
index	String	`default`	The index in which to store the gathered data.
instances	String	`empty`	Instances of a given class for which data is gathered. Specify each instance as a separate argument to the POST operation.
interval	Number		**Required**. The interval, in seconds, at which the WMI provider(s) is queried.
lookup_host	String		**Required**. This is the server from which we is gathering WMI data. If you need to gather data from more than one machine, additional servers can be specified in the 'server' parameter.
name	String		**Required**. This is the name of the collection. This name appears in configuration file, as well as the source and the sourcetype of the indexed data.
server	String	`localhost`	A comma-separated list of additional servers that you want to gather data from. Use this if you need to gather from more than a single machine. See also *lookup_host*.

Returned values

Name	Description
classes	A valid WMI class name.
disabled	Indicates if the input is disabled.
fields	Properties (fields) that you want to gather from the given class.

Name	Description
index	The index in which to store the gathered data.
instances	Instances of a given class for which data is gathered.
interval	The interval, in seconds, at which the WMI provider(s) is queried.
lookup_host	Host from which to monitor log events.
server	Servers from which to gather data. Used if you need to gather from more than a single machine. See also lookup_host.
wql	The actual WQL query for monitoring the performance object.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections -d
classes=Win32_PerfFormattedData_PerfOS_Processor -d interval=5 -d lookup_host=localhost -d name=cpu
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
  <updated>2011-07-27T14:05:43-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>CPUTime</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime</id>
    <updated>2011-07-27T14:05:43-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="index">default</s:key>
        <s:key name="interval">3</s:key>
        <s:key name="wql">SELECT PercentProcessorTime,PercentUserTime FROM
Win32_PerfFormattedData_PerfOS_Processor WHERE Name="_Total"</s:key>
      </s:dict>
    </content>
  </entry>
```

```
</feed>
```

data/inputs/win-wmi-collections/{name}

```
https://<host>:<mPort>/services/data/inputs/win-wmi-collections/{name}
```

Manage the `{name}` WMI collection.

Method summary

Method	Description	Formats
DELETE	Deletes a given collection.	XML, JSON
GET	Gets information about a single collection.	XML, JSON
POST	Modifies a given WMI collection.	XML, JSON

DELETE

Delete a given collection.

Usage details
The method returns HTTP status code = `400`, if `{name}` does not exist.

Request parameters
None

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
  <updated>2011-07-27T14:21:17-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Get information about a single collection.

Request parameters

None

Returned values

Name	Description
classes	A valid WMI class name.
disabled	Indicates if the input is disabled.
fields	Properties (fields) that you want to gather from the given class.
index	The index in which to store the gathered data.
instances	Instances of a given class for which data is gathered.
interval	The interval, in seconds, at which the WMI provider(s) is queried.
lookup_host	Host from which to monitor log events.
name	Collection name. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.
server	Servers frpm which to gather data from. Used if you need to gather from more than a single machine. See also lookup_host.
wql	The actual WQL query for monitoring the performance object.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
```

```
    xmlns:s="http://dev.splunk.com/ns/rest">
<title>win-wmi-collections</title>
<id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
<updated>2011-07-27T14:09:39-07:00</updated>
<generator version="103620"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_new" rel="create"/>
<link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>cpu</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu</id>
  <updated>2011-07-27T14:09:39-07:00</updated>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="list"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="edit"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="remove"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="classes">Win32_PerfFormattedData_PerfOS_Processor</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl node elided ...
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>disabled</s:item>
              <s:item>fields</s:item>
              <s:item>index</s:item>
              <s:item>instances</s:item>
              <s:item>server</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list>
              <s:item>classes</s:item>
              <s:item>interval</s:item>
              <s:item>lookup_host</s:item>
            </s:list>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="fields">
        <s:list>
          <s:item>*</s:item>
        </s:list>
      </s:key>
      <s:key name="index">default</s:key>
      <s:key name="instances">
        <s:list/>
      </s:key>
```

```
        <s:key name="interval">5</s:key>
        <s:key name="lookup_host">localhost</s:key>
        <s:key name="name">cpu</s:key>
        <s:key name="server"/>
        <s:key name="wql">Select * from Win32_PerfFormattedData_PerfOS_Processor</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Modify a collection.

Request parameters

Name	Datatype	Default	Description
classes	String		**Required**. A valid WMI class name.
disabled	Number		Disables the given collection.
fields	String		Properties (fields) that you want to gather from the given class. Specify each property as a separate argument to the POST operation.
index	String		The index in which to store the gathered data.
instances	String		Instances of a given class for which data is gathered. Specify each instance as a separate argument to the POST operation.
interval	Number		**Required**. The interval, in seconds, at which the WMI provider(s) is queried.
lookup_host	String		**Required**. This is the server from which we is gathering WMI data. If you need to gather data from more than one machine, additional servers can be specified in the 'server' parameter.
server	String		A comma-separated list of additional servers that you want to gather data from. Use this if you need to gather from more than a single machine. See also lookup_host parameter.

Returned values

Name	Description
classes	A valid WMI class name.
disabled	Indicates if the input is disabled.
fields	Properties (fields) that you want to gather from the given class.
index	The index in which to store the gathered data.
instances	Instances of a given class for which data is gathered.
interval	The interval, in seconds, at which the WMI provider(s) are queried.
lookup_host	Host from which to monitor log events.

Name	Description
name	Collection name. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.
server	Servers from which to gather data. Used if you need to gather from more than a single machine. See also lookup_host.
wql	The actual WQL query for monitoring the performance object.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu -d
classes=Win32_PerfFormattedData_PerfOS_Processor -d interval=5 -d lookup_host=localhost -d
server=xx.1.5.157,10.1.5.158
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
  <updated>2011-07-27T14:15:33-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>cpu</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu</id>
    <updated>2011-07-27T14:15:33-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="classes">Win32_PerfFormattedData_PerfOS_Processor</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="fields">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="index">default</s:key>
        <s:key name="instances">
```

```
          <s:list/>
        </s:key>
        <s:key name="interval">5</s:key>
        <s:key name="lookup_host">localhost</s:key>
        <s:key name="name">cpu</s:key>
        <s:key name="server"/>
        <s:key name="wql">Select * from Win32_PerfFormattedData_PerfOS_Processor</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/win-perfmon

```
https://<host>:<mPort>/services/data/inputs/win-perfmon
```

Access and manage performance monitoring configurations. This input allows you to poll Windows performance monitor counters.

GET

Get current performance monitoring configuration details.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
counters	List of valid Performance Monitor counters.
disabled	Indicates whether the input is disabled.
index	The index that this input should send data to. If no value is present, send data to the default index.
instances	List of valid instances for a Performance Monitor counter.
interval	How often, in seconds, to poll for new data.
nonmetric_counters	List of valid Performance Monitor counters.
object	A valid Performance Monitor object as defined within Performance Monitor.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/win-perfmon
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-perfmon</title>
  <id>https://10.1.5.157:8089/services/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:42:06-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/services/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Available Memory</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory</id>
    <updated>2011-07-29T19:42:06-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="edit"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory/enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="counters">
          <s:list>
            <s:item>Available Bytes</s:item>
          </s:list>
        </s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="index">default</s:key>
        <s:key name="instances">
          <s:list/>
        </s:key>
        <s:key name="interval">10</s:key>
        <s:key name="object">Memory</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update performance monitoring collection settings.

Request parameters

Name	Datatype	Default	Description
counters	String		A set of counters to monitor. A '*' is equivalent to all counters. Specify each counter as a separate argument to the POST operation.
host	String	Docs-W8R2-Std7	Name of the host for the Windows Performance Monitor.
index	String	default	The index in which to store the gathered data.
instances	String		A set of counter instances to monitor. A '*' is equivalent to all instances. Specify each instance as a separate argument to the POST operation.
interval	Number		How frequently, in seconds, to poll for new data.
name required	String		This is the name of the collection. This name appears in configuration file, as well as the source and the sourcetype of the indexed data.
object	String		A valid performance monitor object (for example, 'Process,' 'Server,' 'PhysicalDisk.')
source	String		Source for inputs.
sourcetype	String		Source type of input.

Returned values

Name	Description
counters	List of valid Performance Monitor counters.
disabled	Indicates whether the input is disabled.
host	Name of the host for the Windows Performance Monitor.
index	The index that this input should send data to. If no value is present, send data to the default index.
instances	List of valid instances for a Performance Monitor counter.
interval	How frequently, in seconds, to poll for new data.
nonmetric_counters	List of valid Performance Monitor counters.
object	A valid Performance Monitor object as defined within Performance Monitor.
source	Source for inputs.
sourcetype	Source type of the input.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon -d interval=4 -d
name=mymemory -d object=Memory
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-perfmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:40:38-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Available Memory</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory</id>
    <updated>2011-07-29T19:40:38-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="counters">Available Bytes</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="instances"/>
        <s:key name="interval">10</s:key>
        <s:key name="object">Memory</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/inputs/win-perfmon/{name}

`https://<host>:<mPort>/services/data/inputs/win-perfmon/{name}`

Manage the `{name}` performance monitoring stanza.

DELETE

Delete a given monitoring stanza.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-perfmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:47:06-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Get settings for a given performance stanza.

Request parameters
None

Returned values

Name	Description
counters	List of valid Performance Monitor counters.
disabled	Indicates whether the input is disabled.
index	The index that this input should send data to. If no value is present, send data to the default index.
instances	List of valid instances for a Performance Monitor counter.

Name	Description
interval	How often, in seconds, to poll for new data.
nonmetric_counters	List of valid Performance Monitor counters.
object	A valid Performance Monitor object as defined within Performance Monitor.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-perfmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:44:21-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>mymemory</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory</id>
    <updated>2011-07-29T19:44:21-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="counters">
          <s:list/>
        </s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>counters</s:item>
                <s:item>disabled</s:item>
                <s:item>index</s:item>
                <s:item>instances</s:item>
                <s:item>interval</s:item>
                <s:item>object</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="index">default</s:key>
        <s:key name="instances">
          <s:list/>
        </s:key>
        <s:key name="interval">4</s:key>
        <s:key name="object">Memory</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Modify an existing monitoring stanza.

Request parameters

Name	Datatype	Default	Description
counters	String		A set of counters to monitor. A '*' is equivalent to all counters. Specify each counter as a separate argument to the POST operation.
host	String	Docs-W8R2-Std7	Name of the host for the Windows Performance Monitor.
index	String	default	The index in which to store the gathered data.
instances	String		A set of counter instances to monitor. A '*' is equivalent to all instances. Specify each instance as a separate argument to the POST operation.
interval	Number		How frequently, in seconds, to poll for new data.
object	String		A valid performance monitor object (for example, 'Process,' 'Server,' 'PhysicalDisk.')
source	String		Source for inputs.
sourcetype	String		Source type of input.

Returned values

Name	Description

Name	Description
counters	List of valid Performance Monitor counters.
disabled	Indicates whether the input is disabled.
host	Name of the host for the Windows Performance Monitor.
index	The index that this input should send data to. If no value is present, send data to the default index.
instances	List of valid instances for a Performance Monitor counter.
interval	How frequently, in seconds, to poll for new data.
nonmetric_counters	List of valid Performance Monitor counters.
object	A valid Performance Monitor object as defined within Performance Monitor,
source	Source for inputs.
sourcetype	Source type of the input.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory -d
interval=10
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-perfmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:45:59-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Available Memory</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory</id>
    <updated>2011-07-29T19:45:59-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="counters">Available Bytes</s:key>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="instances"/>
        <s:key name="interval">10</s:key>
        <s:key name="object">Memory</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/modular-inputs

`https://<host>:<mPort>/services/data/modular-inputs`

Access currently defined modular inputs on the system.

For more information, refer to Modular inputs: Introspection scheme details in *Developing Views and Apps for Splunk Web*.

GET

Get information about configured modular inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
description	Provides descriptive text for title shown on the **Data inputs** manager page. The description also appears on the **Add new data inputs** page.
endpoint	Contains one or more <arg> elements, which define the parameters to an endpoint.
streaming_mode	Indicates the streaming mode for the modular input. Valid values are `xml` and `simple`.
title	The label for a modular input script. The title appears on the **Data inputs** manager page.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/modular-inputs
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>modular-inputs</title>
  <id>https://localhost:8089/services/data/modular-inputs</id>
  <updated>2012-07-09T09:12:41-07:00</updated>
  <generator build="129290" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
   ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>s3</title>
    <id>https://localhost:8089/services/data/modular-inputs/s3</id>
    <updated>2012-07-09T09:12:41-07:00</updated>
    <link href="/services/data/modular-inputs/s3" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/modular-inputs/s3" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description">Get data from Amazon S3.</s:key>
        ... eai:acl node elided ...
        <s:key name="endpoint">
          <s:dict>
            <s:key name="args">
              <s:dict>
                <s:key name="key_id">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Your Amazon key ID.</s:key>
                    <s:key name="order">1</s:key>
                    <s:key name="required_on_create">1</s:key>
                    <s:key name="required_on_edit">0</s:key>
                    <s:key name="title">Key ID</s:key>
                  </s:dict>
                </s:key>
                <s:key name="name">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description"><![CDATA[An S3 resource name without the leading s3://.  For
example, for s3://bucket/file.txt specify bucket/file.txt.  You can also monitor a whole bucket (for example
by specifying 'bucket'), or files within a sub-directory of a bucket (for example 'bucket/some/directory/';
note the trailing slash).]]></s:key>
                    <s:key name="order">0</s:key>
                    <s:key name="title">Resource name</s:key>
                  </s:dict>
                </s:key>
                <s:key name="secret_key">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Your Amazon secret key.</s:key>
                    <s:key name="order">2</s:key>
                    <s:key name="required_on_create">1</s:key>
                    <s:key name="required_on_edit">0</s:key>
                    <s:key name="title">Secret key</s:key>
                  </s:dict>
                </s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="streaming_mode">xml</s:key>
        <s:key name="title">Amazon S3</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>twitter</title>
    <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
    . . . elided . . .
  </entry>
</feed>
```

data/modular-inputs/{name}

`https://<host>:<mPort>/services/data/modular-inputs/{name}`

Get information about the `{name}` modular input.

GET

Get information about a modular input.

Request parameters

None

Returned values

Name	Description
description	The label for a modular input script. The label appears in the **Data inputs** manager page.
endpoint	Contains one or more <arg> elements, which define the parameters to an endpoint.
streaming_mode	Indicates the streaming mode for the modular input. Valid values are `xml` or `simple` (plain text). Contains one or more <arg> elements, which define the parameters to an endpoint.
title	The label for a modular input script. The label appears in the **Data inputs** manager page.

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/data/modular-inputs/twitter
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>modular-inputs</title>
  <id>https://localhost:8089/services/data/modular-inputs</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <generator build="129290" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>twitter</title>
    <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
    <updated>2012-07-09T11:07:29-07:00</updated>
    <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/modular-inputs/twitter" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description">Get data from Twitter.</s:key>
        ... eai:acl and eai:attribute nodes elided ...
        <s:key name="endpoint">
          <s:dict>
            <s:key name="args">
              <s:dict>
                <s:key name="name">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Name of the current feed using the user credentials
supplied.</s:key>
                    <s:key name="order">0</s:key>
                    <s:key name="title">Twitter feed name</s:key>
                  </s:dict>
                </s:key>
                <s:key name="password">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Your twitter password</s:key>
                    <s:key name="order">2</s:key>
                    <s:key name="required_on_create">1</s:key>
                    <s:key name="required_on_edit">0</s:key>
                    <s:key name="title">Password</s:key>
                  </s:dict>
                </s:key>
                <s:key name="username">
                  <s:dict>
                    <s:key name="data_type">string</s:key>
                    <s:key name="description">Your Twitter ID.</s:key>
                    <s:key name="order">1</s:key>
                    <s:key name="required_on_create">1</s:key>
                    <s:key name="required_on_edit">0</s:key>
                    <s:key name="title">Twitter ID/Handle</s:key>
                  </s:dict>
                </s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="streaming_mode">simple</s:key>
        <s:key name="title">Twitter</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

indexing/preview

`https://<host>:<mPort>/services/indexing/preview`

Preview events from a source file before you index the file.

The `edit_monitor` or `edit_upload_and_index` capabilities are required for this endpoint.

GET

Return a list of all data preview jobs.

Usage details

Data returned includes the Splunk management URI to access each preview job.

You can check the status of a data preview job with GET request to `/search/jobs/{search_id}` to obtain information such as the `dispatchState`, `doneProgress`, and `eventCount`. You can also use the data preview job ID as the `search_id` parameter in a GET request to `/search/jobs/{search_id}/results_preview` to preview events from the source file.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/indexing/preview
```

XML Response

```
<title>preview</title>
  <id>https://localhost:8089/services/indexing/preview</id>
  <updated>2011-11-28T14:35:35-08:00</updated>
  <generator version="108769"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>1322518170.8</title>
    <id>https://localhost:8089/services/indexing/preview/1322518170.8</id>
    <updated>2011-11-28T14:35:35-08:00</updated>
    <link href="/services/indexing/preview/1322518170.8" rel="alternate"/>
    <link href="/services/search/jobs/1322518170.8" rel="job"/>
  </entry>
  <entry>
    <title>1322519686.9</title>
    <id>https://localhost:8089/services/indexing/preview/1322519686.9</id>
    <updated>2011-11-28T14:35:35-08:00</updated>
    <link href="/services/indexing/preview/1322519686.9" rel="alternate"/>
    <link href="/services/search/jobs/1322519686.9" rel="job"/>
  </entry>
  <entry>
    <title>1322519724.10</title>
    <id>https://localhost:8089/services/indexing/preview/1322519724.10</id>
    <updated>2011-11-28T14:35:35-08:00</updated>
    <link href="/services/indexing/preview/1322519724.10" rel="alternate"/>
    <link href="/services/search/jobs/1322519724.10" rel="job"/>
  </entry>
```

POST

Create a preview data job for the specified source file, returning the preview data job ID.

Usage details

Typically, you first examine preview data events returned from GET `/search/jobs/{job_id}events`. Then you define new sourcetypes as needed with this endpoint.

Use the POST operation to create a data preview job and return the corresponding data preview job ID. Use the preview job ID as the `search_id` parameter in GET `/search/jobs/{search_id}/results_preview` to obtain a data preview.

You can optionally define sourcetypes for a preview data job in `props.conf`.

Request parameters

Name	Datatype	Default	Description

Name	Datatype	Default	Description
input.path	String		**Required**. The absolute file path to a local file that you want to preview data returned from indexing.
props.<props_attr>	String		Define a new sourcetype in props.conf for preview data that you are indexing.

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/indexing/preview -d
input.path=/Applications/splunk/var/log/splunk/metrics.log
```

XML Response

```
<response>
  <messages>
    <msg type='INFO'>1319496093.11</msg>
  </messages>
</response>
```

indexing/preview/{job_id}

```
https://<host>:<mPort>/services/indexing/preview/{job_id}
```

Get `props.conf` file settings for the `{job_id}` job.

GET

Get `props.conf` file settings for a job.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/services/indexing/preview/1319496093.11
```

XML Response

```
<entry xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
  <title>1319496093.11</title>
  <id>https://localhost:8089/services/indexing/preview/1319496093.11</id>
  <updated>2011-10-24T15:44:09-07:00</updated>
  <link href="/services/indexing/preview/1319496093.11" rel="alternate"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="explicit">
        <s:dict>
          <s:key name="PREFERRED_SOURCETYPE">
            <s:dict>
              <s:key name="value">splunkd</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="inherited">
        <s:dict>
          <s:key name="ANNOTATE_PUNCT">
            <s:dict>
              <s:key name="value">True</s:key>
              <s:key name="stanza">default</s:key>
            </s:dict>
          </s:key>
          . . . elided . . .
          <s:key name="sourcetype">
            <s:dict>
              <s:key name="value">splunkd</s:key>
              <s:key name="stanza">source::.../var/log/splunk/metrics.log(.\d+)?</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
  <link href="/services/search/jobs/1319496093.11" rel="job"/>
</entry>
```

receivers/simple

`https://<host>:<mPort>/services/receivers/simple`
Allows for sending events to Splunk in an HTTP request.

Authentication and authorization

The `edit_tcp` capability is additionally required for this endpoint.

POST

Create events from the contents contained in the HTTP body.

Request parameters

Name	Datatype	Default	Description
<arbitrary_data>	String		**Required**. Raw event text. This is the entirety of the HTTP request body.
host	String		The value to populate in the host field for events from this data input.
host_regex	String		A regular expression used to extract the host value from each event.
index	String	default	The destination index where events are sent.
source	String		The source value to fill in the metadata for this input's events.
sourcetype	String		The sourcetype to apply to events from this input.

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass "https://localhost:8089/services/receivers/simple?source=www&sourcetype=web_event" -d
"Sun Jul 10 15:56:02 PDT 2011   User myusername logged in successfully."
```

XML Response

```
<response>
  <results>
    <result>
      <field k="_index">
        <value>
          <text>default</text>
        </value>
      </field>
      <field k="bytes">
        <value>
          <text>67</text>
        </value>
      </field>
      <field k="host">
        <value>
          <text>127.0.0.1</text>
        </value>
      </field>
      <field k="source">
        <value>
```

```
          <text>www</text>
        </value>
      </field>
      <field k="sourcetype">
        <value>
          <text>web_event</text>
        </value>
      </field>
    </result>
  </results>
</response>
```

receivers/stream

`https://<host>:<mPort>/services/receivers/stream`

Open a socket to receive streaming data.

Authentication and authorization
The `edit_tcp` or `edit_tcp_stream` capabilities are required for this endpoint.

POST

Create events from the stream of data following HTTP headers.

Usage details

Data transfer continues until you enter `<CTRL-C>`.

For streaming connections, set `streaming` and `x-splunk-input-mode` arguments in the header.

For HTTP uploads, if the caller passes a content-type of "multipart/form data", the HTTP file upload protocol is used and files are indexed.

Request parameters

Name	Datatype	Default	Description
<data_stream>	String		**Required**. Raw event text. This does not need to be presented as a complete HTTP request, but can be streamed in as data is available.
host	String		The value to populate in the host field for events from this data input.
host_regex	String		A regular expression used to extract the host value from each event.
index	String		The index to send events from this input to.
source	String		The source value to fill in the metadata for this input's events.
sourcetype	String		The sourcetype to apply to events from this input.

Returned values

None

Example

Python Request

```
import httplib, time

conn = httplib.HTTPSConnection("localhost", 8089)
conn.connect()
conn.putrequest("POST", "/services/receivers/stream?source=www&sourcetype=web_data")
conn.putheader("Authorization", "Splunk 67bed982ce1af9ba2e393b15ed63c916")
conn.putheader("x-splunk-input-mode", "streaming")
conn.endheaders()

i = 0
while i < 100:
   conn.send("%s A sample event (idx: %s).\n" % (time.asctime(), i))
   time.sleep(1)
   i += 1

conn.close()
```

server/pipelinesets

`https://<host>:<mPort>/services/server/pipelinesets`

Provides information on the ingestion pipeline sets on an indexer.

Authentication and authorization

The `list_pipeline_sets` capability is required for this endpoint.

Usage details

See Manage pipeline sets for index parallelization in *Managing Indexers and Clusters of Indexers*.

GET

Query the status of pipeline sets.

Request parameters

None

Returned values

Name	Description
busiest_thread_name	The name of the busiest pipeline thread within the pipeline set for past calculation period.
dutycycle_ratio	The dutycycle ratio of the busiest pipeline thread within the pipeline set for past calculation period.

Name	Description
requests_last_period	The number of ingestion requests processed by the pipeline set in the past calculation period.
share	The relative probability of selection of the pipeline set for the past calculation period.

Example request and response

XML Request

```
curl -k -u admin:changeme https://ronnie:8178/services/server/pipelinesets
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>server-pipeline-sets</title>
  <id>https://ronnie:8178/services/server/pipelinesets</id>
  <updated>2019-02-20T12:24:55-08:00</updated>
  <generator build="62a7f5ca3846ba6f152b123cfab9d4432e97a4a2" version="20190219"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>ingest_pipe_0</title>
    <id>https://ronnie:8178/services/server/pipelinesets/ingest_pipe_0</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/server/pipelinesets/ingest_pipe_0" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/pipelinesets/ingest_pipe_0" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="busiest_thread_name">indexerPipe</s:key>
        <s:key name="dutycycle_ratio">0.0017552064875708618</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="requests_last_period">0</s:key>
      <s:key name="share">1</s:key>
    </s:dict>
  </content>
 </entry>
</feed>
```

services/collector

`<protocol>://<host>:<mPort>/services/collector`

Send events to HTTP Event Collector using the Splunk platform JSON event protocol.

By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Note: When using an ACK-enabled token, an `ackID` is returned within a JSON object in the response. For example, `{"ackID": "0"}` indicates an ackID of 0. Use the `ackID` to query the `services/collector/ack` endpoint to verify event indexing. For more information, see services/collector/ack.

Authorization

Requires an HTTP Event Collector token or basic auth, as defined in RFC 1945. See request examples for more details.

See also

- data/inputs/http
- data/inputs/http/{name}
- data/inputs/http/{name}/disable
- data/inputs/http/{name}/enable

POST

Send events to the HTTP Event Collector.

Usage details

HTTP Event Collector functionality must be enabled to send events.

To send events to the HTTP Event Collector, you must provide an HTTP Event Collector token in the authorization header. The token is created using the `data/inputs/http` endpoint. You can then retrieve the token with a GET request on the `data/inputs/http/{name}` endpoint, where `{name}` is the name of your token. Include the authentication token in the request header using the following format: `Authorization: Splunk <token>`. The format is case-sensitive.

Use the Splunk search application to view the logged events. For example, use `index=main | search sourcetype=access` to view all logged events with a sourcetype of access.

For performance reasons, the data input endpoint follows a simple error handling model. It assumes that in most cases it receives a well-formed event data payload. If there is malformed event data in the payload, events continue to be extracted until an error is encountered. Processing stops immediately on an error and the error and number of payload events processed successfully are reported. Events processed before the error are sent to indexers and all events after the first error are dropped.

Request parameters

Name	Datatype	Description
channel	See description	Required if `useAck` is enabled. Pass in the channel GUID as a string parameter or using the `"x-splunk-request-channel"` header.
event	string	Required. Event payload key-value. Value can be a string or a JSON object. JSON example: `{"event": {"message":"Access log test message"}}` String example: `"event": "Access log test message."`
fields	JSON object	Fields for indexing that do not occur in the event payload itself. You can use this parameter when you do not want particular fields to be included in the event data, but you need additional metadata for indexing and searching. Specify one or more additional fields to include for indexing with the event payload. For each field, use a key to specify the name and include one or more values. Specify multiple values in an array. In the following example, the `"severity"` field gets the value `"INFO"` and the `"category"` key gets both `"foo"` and `"bar"` values. `-d {"event": "something happened", "fields": {"severity": "INFO", "category": ["foo", "bar"]}}`
host	string	Host name. Specify with the *host* query string parameter. Sets a default for all events in the request. The default host name can be overridden.
index	string	Index name. Specify with the *index* query string parameter. Sets a default for all events in the request. The default index name can be overridden.
source	string	User-defined event source. Specify with the *source* query string parameter. Sets a default for all events in the request. The default source can be overridden.
sourcetype	string	User-defined event sourcetype. Specify with the *sourcetype* query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.
time	string or unsigned integer	Epoch-formatted time. Specify with the *time* query string parameter. Sets a default for all events in the request. The default time can be overridden. For more information about formatting, see Format events for HTTP Event Collector.

Returned values

Name	Description
text	Human readable status, same value as *code*.
code	Machine format status, same value as *text*.
invalid-event-number	When errors occur, indicates the zero-based index of first invalid event in an event sequence.
ackId	If `useACK` is enabled for the token, indicates the `ackId` to use for checking an indexer acknowledgement.

Response status codes

The following status codes have particular meaning for all HTTP Event Collector endpoints:

Status Code	HTTP status code ID	HTTP status code	Status message
0	200	OK	`Success`
1	403	Forbidden	`Token disabled`
2	401	Unauthorized	`Token is required`
3	401	Unauthorized	`Invalid authorization`
4	403	Forbidden	`Invalid token`
5	400	Bad Request	`No data`
6	400	Bad Request	`Invalid data format`
7	400	Bad Request	`Incorrect index`
8	500	Internal Error	`Internal server error`
9	503	Service Unavailable	`Server is busy`
10	400	Bad Request	`Data channel is missing`
11	400	Bad Request	`Invalid data channel`
12	400	Bad Request	`Event field is required`
13	400	Bad Request	`Event field cannot be blank`
14	400	Bad Request	`ACK is disabled`
15	400	Bad Request	`Error in handling indexed fields`
16	400	Bad Request	`Query string authorization is not enabled`

Example response messages

Success:

```
    {"text":"Success","code":0}
```

Failure:

```
    {"text":"Incorrect data format","code":5,"invalid-event-number":0}
```

Example request and response

JSON Request

```
curl https://localhost:8089/services/collector -H 'Authorization: Splunk
3DEA16E1-413A-46C2-A74F-E79DC3DF3CA2' -d '{"sourcetype":"access", "source":"/var/log/access.log", "event":
{"message":"Access log test message"}} {"sourcetype":"access", "source":"/var/log/access.log", "event":
{"message":"Access log test message 2"}}'
```

JSON Response

```
{"text":"Success","code":0}
```

JSON Response

For `index=main | search sourcetype=access`

```
Time                 Event
1/26/15
10:07:09.000 PM
                { [-]
                   message: Access log test message 2
                }

1/26/15
10:07:09.000 PM
                { [-]
                   message: Access log test message
                }
```

Request including the fields parameter

```
curl https://localhost:8088/services/collector?
-H 'Authorization: Splunk 46931F1C-352C-4DF6-820C-F2689CF88494'
-d '{"event":"something happened", "fields":{"severity":"INFO", "category":["foo","bar"]}}'
```

Basic auth request

```
curl -u x:46931F1C-352C-4DF6-820C-F2689CF88494
https://localhost:8088/services/collector/JSON
-d 'Hello World'
```

services/collector/ack

```
<protocol>://<host>:<mPort>/services/collector/ack
```

Query event indexing status.

For events sent using HTTP Event Collector, check event indexing status. Requests must use a valid channel ID and authorization token with `useACK` enabled. An event ACK ID, returned in response to a POST to `services/collector`, is also required.

By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Authentication and authorization

Requires an HTTP Event Collector *`<Token>`*.

GET

Get HTTP Event Collector event indexing status.

Request parameters

Parameter	Datatype	Description
channel	See description	Required. Pass in the channel GUID as the *channel* string parameter or using the `x-splunk-request-channel` header.
`"acks"`	JSON object	Required. JSON object with an array of ack ID values. Include in the request payload.

Returned values

Name	Description
acks	Contains the key/value pairs for each ACK ID requested. For each key in the `"acks"` object, a `true` value means the ACK ID's events were indexed. A `false` value means that indexing status is unknown. For example, an event may have an indexing delay long enough that it is no longer tracked. Here is an example response. `{"acks" : { "0" : true, "1" : false, "2" : true, "3" : false}}`

Response status codes

Several HTTP status codes have particular meaning for all HTTP Event Collector endpoints. See HTTP Status Codes in services/collector.

Example requests and responses

For application token = `B48F6736-479F-486B-96F9-3EF8C6378E70`.

Note: `useACK` must be enabled on the token for use with this endpoint.

JSON request

```
curl https://localhost:8088/services/collector/ack?channel=2AC79941-CB26-421C-8826-F57AE23E9702 -H
"Authorization: Splunk B48F6736-479F-486B-96F9-3EF8C6378E70" -d '{"acks":[0,1]}'
```

JSON response body

```
{"acks":{"0":true,"1":true}}
```

services/collector/event

Sends timestamped events to HTTP Event Collector using the Splunk platform JSON event protocol when `auto_extract_timestamp` is set to "true" in the /event URL.

- An example of a timestamp is: 2017-01-02 00:00:00.
- If there is a timestamp in the event's JSON envelope, Splunk honors that timestamp first.
- If there is no timestamp in the event's JSON envelope, the merging pipeline extracts the timestamp from the event.
- If "time=xxx" is used in the /event URL then `auto_extract_timestamp` is disabled.
- Splunk supports timestamps using the Epoch format.

services/collector/event/1.0

This endpoint works identically to services/collector/event but introduces a protocol version for future scalability. For more information, see services/collector.

services/collector/health

```
<protocol>://<host>:8088/services/collector/health
```

This endpoint checks if HEC is healthy and able to accept new data from a load balancer.

When there is no optional parameter defined, the default query string is `services/collector/health`. In this case, the service will check the status of the HttpInputQueue for all tokens.

When ack is defined, the query string is either set to `services/collector/health?ack=true` or `services/collector/health?ack=1`.The service will check the status of the HttpInputQueue for all tokens, and the overall health of the AckService.

When a token is defined, the query string is set to `services/collector/health?token=<token>`. The service will check whether HttpInputQueue is able to accept further data using that specific token.

When both a token and ack are defined, the query string is set to `services/collector/health?ack=true&token=<token>`. The service will check whether HttpInputQueue is able to accept further data using that specific token, and the overall health of the AckService. This operation will run even if ack is disabled for the specified token. To check whether a specific token has ack enabled or disabled, see About HTTP Event Collector Indexer Acknowledgment in the *Getting Data In* manual to learn more about useAck status.

In this context, the overall health of the AckService refers to checking three things:

- `max_number_of_acked_requests_pending_query_per_ack_channel`: the number of acks inside each channel
    - If backpressureState is `disabled` (which is the default and existing state), the AckService is unhealthy when at least one channel is full.
    - If backpressureState is `warn_at_80`, the AckService is unhealthy when every channel is full.
- `max_number_of_ack_channel`: maximum number of ack channels
    - ack is unhealthy when the number of channels meets or exceeds this number
- max_number_of_acked_requests_pending_query: number of acks across all channels
    - ack is unhealthy when the number of pending requests meets or exceeds this number

Usage details

Port and protocol

By default, this endpoint works on port 8088 and uses HTTPS for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Response codes

Status Code	Description
200	HEC is available and accepting input
17	HEC is available and accepting input
503	HEC is unhealthy, queues are full

services/collector/health/1.0

`<protocol>://<host>:8088/services/collector/health/1.0`

This endpoint checks if HEC is healthy and able to accept new data from a load balancer. HEC health is determined if there is space available in the queue.

This endpoint works identically to `services/health` but introduces a protocol version for future scalability. For more information, see services/collector/health.

Usage details

Port and protocol

By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Response codes

Status Code	Description
200	HEC is available and accepting input
17	HEC is available and accepting input
503	HEC is unhealthy, queues are full

services/collector/mint

`<protocol>://<host>:<mPort>/services/collector/mint`

Post MINT formatted data to the HTTP Event Collector. The authorization header contains the authorization scheme and application token. The HTTP POST body contains event data in the MINT payload format.

Authentication and authorization

Requires an HTTP Event Collector `<token>`.

Note: By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

POST

Post MINT formatted data.

Request parameters

Name	Datatype	Description
host	String	Host name. Specify with the *host* query string parameter. Sets a default for all events in the request. Can be overridden.
index	String	Index name. Specify with the *index* query string parameter. Sets a default for all events in the request. Can be overridden.
source	String	User-defined event source. Specify with the *source* query string parameter. Sets a default for all events in the request. The default source can be overridden.
sourcetype	string	User-defined event sourcetype. Specify with the *sourcetype* query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.
time	string or unsigned integer	Epoch-formatted time. Specify with the *time* query string parameter. Sets a default for all events in the request. The default time can be overridden.

Returned values

None

Response status codes

Several HTTP status codes have particular meaning for all HTTP Event Collector endpoints. See HTTP Status Codes in services/collector.

Example request and response

Observe that the POST request is made to port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

MINT

For application token = `B5A79AAD-D822-46CC-80D1-819F80D7BFB0`

MINT Request

```
curl http://localhost:8088/services/collector/mint -H 'Authorization: Splunk
B5A79AAD-D822-46CC-80D1-819F80D7BFB0' -d '{"data":"hello"}{^1^log^1433256}'
```

services/collector/mint/1.0

This endpoint works identically to receivers/token/mint but introduces a protocol version for future scalability.

[Top]

services/collector/raw

`<protocol>://<host>:<mPort>/services/collector/raw`

Send raw data directly to the HTTP Event Collector. This endpoint allows one or more raw events to be sent in a single request. Events are parsed using regex or JSON extraction. JSON field extraction works at index time.

Usage details

Channel

This endpoint requires a data channel GUID to differentiate data from different clients. Generate a GUID and provide it in a POST request as a custom HTTP header or as a parameter.

If a channel is not provided in the POST request, an error response is sent. Only valid GUIDs can be used. An error message is returned if GUID validation fails.

Port and protocol

By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Authentication and authorization

Requires an HTTP Event Collector token or basic auth, as defined in RFC 1945. See request examples for more details.

POST

Send raw data to the to the indexer queue. Requires a data channel GUID, provided as a custom HTTP header or request parameter.

Request parameters

Name	Datatype	Description
channel	See description.	**Required**. Pass in the channel GUID as the *channel* string parameter or using the `x-splunk-request-channel` header.
host	String	Host name. Specify with the *host* query string parameter. Sets a default for all events in the request. Can be overridden.
index	String	Index name. Specify with the *index* query string parameter. Sets a default for all events in the request. Can be overridden.
source	String	User-defined event source. Specify with the *source* query string parameter. Sets a default for all events in the request. The default source can be overridden.
sourcetype	string	User-defined event sourcetype. Specify with the *sourcetype* query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.
time	string or unsigned integer	Epoch-formatted time. Specify with the *time* query string parameter. Sets a default for all events in the request. The default time can be overridden.

Returned values

None

Response status codes
Several HTTP status codes have particular meaning for all HTTP Event Collector endpoints. See HTTP Status Codes in services/collector.

Example request and response

Note that the following POST request examples are made to port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Simple request
This example passes the channel ID as part of the header.

```
curl  https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAACEFBC4AB -H
"Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BFB0" -d 'Hello World'}'
```

Request including a timestamp

```
curl  https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAACEFBC4AB
-H 'Authorization: Splunk 934793C0-FC91-467E-965A-7EAACEFBC4AB'
-d 'Wed Aug 10 12:27:53 PDT 2016 Hello World'
```

JSON request with timestamp

```
curl  https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAACEFBC4AB
-H 'Authorization: Splunk 934793C0-FC91-467E-965A-7EAACEFBC4AB'
-d '{"message":"Hello World", "date":"Wed Aug 10 12:27:53 PDT 2016"}'
```

Basic auth request

```
curl -u x:46931F1C-352C-4DF6-820C-F2689CF88494
https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAACEFBC4AB
-d 'Hello World'
```

Example JSON Response

```
{"text":"Success","code":0}
```

services/collector/raw/1.0

This endpoint works identically to `services/collector/raw` but introduces a protocol version for future scalability. See services/collector/raw.

services/collector/s2s

Compatible with Splunk Enterprise versions 8.1.0 and higher

`<protocol>://<host>:8088/services/collector/s2s`

This endpoint receives Splunk TCP data over HTTP from the Splunk Universal Forwarder. Compatible with Splunk 8.1.0 and later.

Usage details

Port and protocol

By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Response codes

Status Code	Description
200	HEC is available and accepting input
400	Invalid HEC token
503	HEC is unhealthy, queues are full

Introspection endpoints

Introspection endpoint descriptions

Access server and instance information.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud limitations

If you have a managed Splunk Cloud deployment with search head clustering and index clustering, the REST API supports access to the search head only. You can use the REST API to interact with the search head in your deployment. Using the REST API to access any other cluster member nodes is not supported. For example, introspection endpoints are not applicable to Splunk Cloud deployments.

---

data/index-volumes

`https://<host>:<mPort>/services/data/index-volumes`

Get information about the volume (logical drives) in use by the Splunk deployment.

GET

List the Splunk deployment volumes.

Usage details

The default update period is 10 minutes, as defined by the `collectionPeriodInSecs` attribute in the following file.

```
$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf
```

At least one observation period must pass after Splunk software startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
max_size	Maximum *name* volume size limit (MB): `infinite` = No maximum specified.
name	Volume name
total_size	Total *name* volume capacity (MB). If *max_size* is `infinite`, this field is not listed.

Example request and response

XML Request

```
curl -k -u admin:passwd https://localhost:8089/services/data/index-volumes
```

XML Response

```
...
<title>introspection--disk-objects--volumes</title>
 <id>https://localhost:8089/services/data/index-volumes</id>
 <updated>2014-03-25T14:41:09-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>_splunk_summaries</title>
   <id>https://localhost:8089/services/data/index-volumes/_splunk_summaries</id>
   <updated>2014-03-25T14:41:09-07:00</updated>
   <link href="/services/data/index-volumes/_splunk_summaries" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/data/index-volumes/_splunk_summaries" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
```

```
        ... elided ...
      </s:key>
      <s:key name="max_size">infinite</s:key>
      <s:key name="name">_splunk_summaries</s:key>
    </s:dict>
  </content>
</entry>
```

data/index-volumes/{name}

`https://<host>:<mPort>/services/data/index-volumes/{name}`

Get information about the `{name}` volume (logical drive).

GET

List `{name}` volume properties.

Usage details

The default update period is 10 minutes, as defined by the `collectionPeriodInSecs` attribute in the following file.

`$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf`

At least one observation period must pass after Splunk software startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
max_size	Maximum *name* volume size limit (MB). `infinite` = No maximum specified (i.e., 0, the default)
name	Volume name.
total_size	Total *name* volume capacity (MB). If *max_size* is `infinite`, this field is not listed.

Example request and response

XML Request

```
curl -k -u admin:passwd https://localhost:8089/services/data/index-volumes/_splunk_summaries
```

XML Response

```
...
 <title>introspection--disk-objects--volumes</title>
 <id>https://localhost:8089/services/data/index-volumes</id>
 <updated>2014-03-27T14:35:26-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>_splunk_summaries</title>
   <id>https://localhost:8089/services/data/index-volumes/_splunk_summaries</id>
   <updated>2014-03-27T14:35:26-07:00</updated>
   <link href="/services/data/index-volumes/_splunk_summaries" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/data/index-volumes/_splunk_summaries" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="eai:attributes">... elided ...</s:key>
       <s:key name="max_size">infinite</s:key>
       <s:key name="name">_splunk_summaries</s:key>
     </s:dict>
   </content>
 </entry>
```

data/indexes

`https://<host>:<mPort>/services/data/indexes`
Create and manage data indexes.

Authorization and authentication

By default, all users can list all indexes. However, if the `indexes_list_all` capability is enabled in `authorize.conf`, access to all indexes is limited to only those roles with this capability.

To enable `indexes_list_all` capability restrictions on the `data/indexes` endpoint, create a `[capability::indexes_list_all]` stanza in `authorize.conf`. Specify `indexes_list_all=enabled` for any role permitted to list all indexes from this endpoint.

For more information, see the authorize.conf spec file in the *Admin Manual*.

GET

List the recognized indexes on the server.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Type	Default	Description
datatype	String	event	Valid values: (all | event | metric). Specifies the type of index.

Returned values

Name	Description
assureUTF8	Indicates whether all data retreived from the index is proper UTF8. If enabled (set to True), degrades indexing performance. This is a global setting, not a per index setting.
blockSignSize	Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.
blockSignatureDatabase	The index that stores block signatures of events. This is a global setting, not a per index setting.
coldPath	Filepath to the cold databases for the index.
coldPath_expanded	Absoute filepath to the cold databases.
coldToFrozenDir	Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory. Bucket freezing policy is as follows: • New style buckets (4.2 and on): removes all files but the rawdata To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory • Old style buckets (Pre-4.2): gzip all the .data and .tsidx files To thaw, unzip the zipped files and move the bucket into the thawed directory If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.
coldToFrozenScript	Path to the archiving script. See the POST parameter description for details.
compressRawdata	This value is ignored. splunkd process always compresses raw data.
currentDBSizeMB	Total size, in MB, of data stored in the index. The total incudes data in the home, cold and thawed paths.
datatype	The type of index (event | metric).
defaultDatabase	

Name	Description
	If no index destination information is available in the input data, the index shown here is the destination of such data.
disabled	Indicates if the index is disabled.
enableRealtimeSearch	Indicates if this is a real-time search. This is a global setting, not a per index setting.
frozenTimePeriodInSecs	Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years). Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.
homePath	An absolute path that contains the hot and warm buckets for the index.
homePath_expanded	An absolute filepath to the hot and warm buckets for the index.
indexThreads	Number of threads used for indexing. This is a global setting, not a per index setting.
isInternal	Indicates if this is an internal index (for example, _internal, _audit).
isReady	Indicates if the index is properly initialized.
lastInitTime	Last time the index processor was successfully initialized. This is a global setting, not a per index setting.
maxConcurrentOptimizes	The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
maxDataSize	The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended). Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" is typically one that gets over 10GB of data per day. • "auto" sets the size to 750MB. • "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems. Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. *Note:* The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.
maxHotBuckets	Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs,

Name	Description
	which can also cause hot buckets to roll.
maxHotIdleSecs	Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time). If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.
maxHotSpanSecs	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). *Note:* If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.
maxMemMB	The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting.
maxMetaEntries	Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.
maxRunningProcessGroups	Maximum number of processes that the indexer fires off at a time. This is a global setting, not a per index setting.
maxTime	ISO8601 timestamp of the newest event time in the index.
maxTotalDataSizeMB	The maximum size of an index, in MB.
maxWarmDBCount	The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.
memPoolMB	Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.
minRawFileSyncSecs	Can be either an integer (or "disable"). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files.

Name	Description
	If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying "disable" disables syncing entirely: uncompressed slices are removed as soon as compression is complete.
minTime	ISO8601 timestamp of the oldest event time in the index.
partialServiceMetaPeriod	Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every <integer> seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.
quarantineFutureSecs	Events with timestamp of `quarantineFutureSecs` newer than "now" that are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.
quarantinePastSecs	Events with timestamp of quarantinePastSecs older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.
rawChunkSizeBytes	Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. *Note:* rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. *Warning:* This is an advanced parameter. Only change it if instructed to do so by Splunk Support.
rotatePeriodInSecs	Rotation period, in seconds, that specifies how frequently to check: • If a new hot bucket needs to be created. • If there are any cold buckets that should be frozen. • If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.
serviceMetaPeriod	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.
summarize	If true, leaves out certain index details, which provides a faster response.
suppressBannerList	List of indexes for which we suppress "index missing" warning banner messages.

Name	Description
	This is a global setting, not a per index setting.
sync	Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.
syncMeta	When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. *Note:* Do not change this parameter without the input of Splunk Support.
thawedPath	An absolute path that contains the thawed (resurrected) databases for the index.
thawedPath_expanded	Absolute filepath to the thawed (resurrected) databases.
throttleCheckPeriod	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). *Note:* Do not change this parameter without the input of Splunk Support.
totalEventCount	Total number of events in the index.
tsidxDedupPostingsListMaxTermsLimit	This setting is valid only when `tsidxWritingLevel` is at 4 or higher. This maximum term limit sets an upper bound on the number of terms kept inside an in-memory hash table that serves to improve tsidx compression. The tsidx optimizer uses the hash table to identify terms with identical postings lists. When the first instance of a term is received, its postings list is stored. When successive terms with identical postings lists are received, the tsidx optimizer makes them refer to the first instance of the postings list rather than creating and storing term postings list duplicates. Consider increasing this limit to improve compression for large tsidx files. For example, a tsidx file created with `tsidxTargetSizeMB` over 1500MB can contain a large number of terms with identical postings lists. Reducing this limit helps conserve memory consumed by optimization processes, at the cost of reduced tsidx compression. Set this limit to 0 to disable deduplicated postings list compression. This setting cannot exceed 1,073,741,824 (2^{30}). Defaults to 8,388,608 (2^{23}).

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/data/indexes
```

XML Response

```
.
.
.
<title>indexes</title>
 <id>https://localhost:8089/services/data/indexes</id>
 <updated>2011-07-11T18:09:22-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
```

```
</author>
<link href="/services/data/indexes/_new" rel="create"/>
<link href="/services/data/indexes/_reload" rel="_reload"/>
   ... opensearch elements elided ...
<s:messages/>
<entry>
  <title>_audit</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/indexes/_audit</id>
  <updated>2011-07-11T18:09:22-07:00</updated>
  <link href="/servicesNS/nobody/system/data/indexes/_audit" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/indexes/_audit" rel="list"/>
  <link href="/servicesNS/nobody/system/data/indexes/_audit/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/indexes/_audit" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/indexes/_audit/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="assureUTF8">0</s:key>
      <s:key name="blockSignSize">0</s:key>
      <s:key name="blockSignatureDatabase">_blocksignature</s:key>
      <s:key name="coldPath">$SPLUNK_DB/audit/colddb</s:key>
      <s:key name="coldPath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/colddb</s:key>
      <s:key name="coldToFrozenDir"/>
      <s:key name="coldToFrozenScript"/>
      <s:key name="compressRawdata">1</s:key>
      <s:key name="currentDBSizeMB">1</s:key>
      <s:key name="datatype">event</s:key>
      <s:key name="defaultDatabase">main</s:key>
      <s:key name="disabled">0</s:key>
         ... eai:acl element elided ...
      <s:key name="enableRealtimeSearch">1</s:key>
      <s:key name="frozenTimePeriodInSecs">188697600</s:key>
      <s:key name="homePath">$SPLUNK_DB/audit/db</s:key>
      <s:key name="homePath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/db</s:key>
      <s:key name="indexThreads">auto</s:key>
      <s:key name="isInternal">1</s:key>
      <s:key name="lastInitTime">1310432962.424512</s:key>
      <s:key name="maxConcurrentOptimizes">3</s:key>
      <s:key name="maxDataSize">auto</s:key>
      <s:key name="maxHotBuckets">3</s:key>
      <s:key name="maxHotIdleSecs">0</s:key>
      <s:key name="maxHotSpanSecs">7776000</s:key>
      <s:key name="maxMemMB">5</s:key>
      <s:key name="maxMetaEntries">1000000</s:key>
      <s:key name="maxRunningProcessGroups">20</s:key>
      <s:key name="maxTime">2011-07-10T22:20:53-0700</s:key>
      <s:key name="maxTotalDataSizeMB">500000</s:key>
      <s:key name="maxWarmDBCount">300</s:key>
      <s:key name="memPoolMB">auto</s:key>
      <s:key name="minRawFileSyncSecs">disable</s:key>
      <s:key name="minTime">2011-07-10T14:33:00-0700</s:key>
      <s:key name="partialServiceMetaPeriod">0</s:key>
      <s:key name="quarantineFutureSecs">2592000</s:key>
      <s:key name="quarantinePastSecs">77760000</s:key>
      <s:key name="rawChunkSizeBytes">131072</s:key>
      <s:key name="rotatePeriodInSecs">60</s:key>
      <s:key name="serviceMetaPeriod">25</s:key>
      <s:key name="suppressBannerList"/>
      <s:key name="sync">0</s:key>
      <s:key name="syncMeta">1</s:key>
```

```
       <s:key name="thawedPath">$SPLUNK_DB/audit/thaweddb</s:key>
       <s:key name="thawedPath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/thaweddb</s:key>
       <s:key name="throttleCheckPeriod">15</s:key>
       <s:key name="totalEventCount">230</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Create a new index.

Request parameters

Name	Type	Default	Description
blockSignSize	Number	0	Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.
bucketRebuildMemoryHint	String	auto	Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make. *Caution:* This is an advanced parameter. Inappropriate use of this parameter causes splunkd to not start if rebuild is required. *Do not set this parameter unless instructed by Splunk Support.* Default value, `auto`, varies by the amount of physical RAM on the host • less than 2GB RAM = 67108864 (64MB) tsidx • 2GB to 8GB RAM = 134217728 (128MB) tsidx • more than 8GB RAM = 268435456 (256MB) tsidx Values other than "auto" must be 16MB-1GB. Highest legal value (of the numerical part) is 4294967295 You can specify the value using a size suffix: "16777216" or "16MB" are equivalent.
coldPath	String		An absolute path that contains the colddbs for the index. The path must be readable and writable. Cold databases are opened as needed when searching. May be defined in terms of a volume definition (see volume section below). Required. Splunk software does not start if an index lacks a valid coldPath.
coldToFrozenDir	String		Destination path for the frozen archive. Use as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory. Bucket freezing policy is as follows: • New style buckets (4.2 and on): removes all files but the rawdata To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory

Name	Type	Default	Description
			- Old style buckets (Pre-4.2): gzip all the .data and .tsidx files To thaw, gunzip the zipped files and move the bucket into the thawed directory If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence
coldToFrozenScript	String		Path to the archiving script. If your script requires a program to run it (for example, python), specify the program followed by the path. The script must be in $SPLUNK_HOME/bin or one of its subdirectories. Splunk software ships with an example archiving script in $SPLUNK_HOME/bin called coldToFrozenExample.py. DO NOT use this example script directly. It uses a default path, and if modified in place any changes are overwritten on upgrade. It is best to copy the example script to a new file in bin and modify it for your system. Most importantly, change the default archive path to an existing directory that fits your needs. If your new script in bin/ is named myColdToFrozen.py, set this key to the following: `coldToFrozenScript = "$SPLUNK_HOME/bin/python" "$SPLUNK_HOME/bin/myColdToFrozen.py"` By default, the example script has two possible behaviors when archiving: - For buckets created from version 4.2 and on, it removes all files except for rawdata. To thaw: cd to the frozen bucket and type `splunk rebuild .`, then copy the bucket to thawed for that index. We recommend using the coldToFrozenDir parameter unless you need to perform a more advanced operation upon freezing buckets. - For older-style buckets, we simply gzip all the .tsidx files. To thaw: cd to the frozen bucket and unzip the tsidx files, then copy the bucket to thawed for that index
compressRawdata	Boolean	true	This parameter is ignored. The splunkd process always compresses raw data.
datatype	String	event	Valid values: (event | metric). Specifies the type of index.
enableOnlineBucketRepair	Boolean	true	Enables asynchronous "online fsck" bucket repair, which runs concurrently with Splunk software. When enabled, you do not have to wait until buckets are repaired to start the Splunk platform. However, you might observe a slight performance degratation.
frozenTimePeriodInSecs	Number	188697600	Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).

Name	Type	Default	Description
			Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.
homePath	String		An absolute path that contains the hot and warm buckets for the index. Required. Splunk software does not start if an index lacks a valid homePath. **Caution:** The path must be readable and writable.
maxBloomBackfillBucketAge	Number	30d	Valid values are: Integer[m|s|h|d] If a warm or cold bucket is older than the specified age, do not create or rebuild its bloomfilter. Specify 0 to never rebuild bloomfilters. For example, if a bucket is older than specified with maxBloomBackfillBucketAge, and the rebuilding of its bloomfilter started but did not finish, do not rebuild it.
maxConcurrentOptimizes	Number	6	The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
maxDataSize	Number	auto	The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended).Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" would typically be considered one that gets over 10GB of data per day. • "auto" sets the size to 750MB. • "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems. Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. *Note:* The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.
maxHotBuckets	Number	3	Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.

Name	Type	Default	Description
maxHotIdleSecs	Number	0	Maximum life, in seconds, of a hot bucket. Defaults to 0. If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll. A value of 0 turns off the idle check (equivalent to INFINITE idle time).
maxHotSpanSecs	Number	7776000	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). *Note:*I f you set this too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.
maxMemMB	Number	5	The amount of memory, expressed in MB, to allocate for buffering a single tsidx file into memory before flushing to disk. Defaults to 5. The default is recommended for all environments. IMPORTANT: Calculate this number carefully. Setting this number incorrectly may have adverse effects on your systems memory and/or splunkd stability/performance.
maxMetaEntries	Number	1000000	Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the `punct` field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.
maxTimeUnreplicatedNoAcks	Number	300	Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored. If there are any acknowledged events sharing this raw slice, this paramater does not apply. In this case, maxTimeUnreplicatedWithAcks applies. Highest legal value is 2147483647. To disable this parameter, set to 0. *Note:* this is an advanced parameter. Understand the consequences before changing.
maxTimeUnreplicatedWithAcks	Number	60	Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering).

Name	Type	Default	Description
			Note: This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.
maxTotalDataSizeMB	Number	500000	The maximum size of an index (in MB). If an index grows larger than the maximum size, the oldest data is frozen.
maxWarmDBCount	Number	300	The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times is moved to cold.
minRawFileSyncSecs	Number	disable	Specify an integer (or "disable") for this parameter. This parameter sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying "disable" disables syncing entirely: uncompressed slices are removed as soon as compression is complete. *Note:* Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed
minStreamGroupQueueSize	Number	2000	Minimum size of the queue that stores events in memory before committing them to a tsidx file. *Caution*: Do not set this value, except under advice from Splunk Support.
name required	String		The name of the index to create.
partialServiceMetaPeriod	Number	0	Related to serviceMetaPeriod. If set, it enables metadata sync every <integer> seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. `partialServiceMetaPeriod` specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect. By default it is turned off (zero).

Name	Type	Default	Description
processTrackerServiceInterval	Number	1	Specifies, in seconds, how often the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests. Defaults to 15. If set to 0, the indexer checks child process status every second. Highest legal value is 4294967295.
quarantineFutureSecs	Number	2592000	Events with timestamp of `quarantineFutureSecs` newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.
quarantinePastSecs	Number	77760000	Events with timestamp of `quarantinePastSecs` older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.
rawChunkSizeBytes	Number	131072	Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, `rawChunkSizeBytes` is set to the default value. *Note:* rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. WARNING: This is an advanced parameter. Only change it if you are instructed to do so by Splunk Support.
repFactor	String	0	Index replication control. This parameter applies to only clustering slaves. `auto` = Use the master index replication configuration value. `0` = Turn off replication for this index.
rotatePeriodInSecs	Number	60	How frequently (in seconds) to check if a new hot bucket needs to be created. Also, how frequently to check if there are any warm/cold buckets that should be rolled/frozen.
serviceMetaPeriod	Number	25	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.
syncMeta	Boolean	true	When `true`, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. **Note**: Do not change this parameter without the input of a Splunk Support.
thawedPath	String		An absolute path that contains the thawed (resurrected) databases for the index.

Name	Type	Default	Description
			Cannot be defined in terms of a volume definition. Required. Splunk software does not start if an index lacks a valid `thawedPath`.
throttleCheckPeriod	Number	15	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). **Note**: Do not change this parameter without the input of Splunk Support.
tstatsHomePath	String		Location to store datamodel acceleration TSIDX data for this index. Restart splunkd after changing this parameter. If specified, it must be defined in terms of a volume definition. *Caution*: Path must be writable. *Default value*: volume:_splunk_summaries/$_index_name/tstats
warmToColdScript	String		Path to a script to run when moving data from warm to cold. This attribute is supported for backwards compatibility with Splunk software versions older than 4.0. Contact Splunk support if you need help configuring this setting. *Caution*: Migrating data across filesystems is now handled natively by splunkd. If you specify a script here, the script becomes responsible for moving the event data, and Splunk-native data migration is not used.

Returned values

Name	Description
assureUTF8	Boolean value indicating wheter all data retreived from the index is proper UTF8. If enabled (set to True), degrades indexing performance Can only be set globally.
blockSignSize	Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.
blockSignatureDatabase	The index that stores block signatures of events. This is a global setting, not a per index setting.
bucketRebuildMemoryHint	Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.

Name	Description
coldPath	Filepath to the cold databases for the index.
coldPath_expanded	Absoute filepath to the cold databases.
coldToFrozenDir	Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory. Bucket freezing policy is as follows: • New style buckets (4.2 and on): removes all files but the rawdata To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory • Old style buckets (Pre-4.2): gzip all the .data and .tsidx files To thaw, unzip the zipped files and move the bucket into the thawed directory If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.
coldToFrozenScript	Path to the archiving script. See the POST parameter description for details.
compressRawdata	This value is ignored. splunkd process always compresses raw data.
currentDBSizeMB	Total size, in MB, of data stored in the index. The total incudes data in the home, cold and thawed paths.
datatype	The type of index (event | metric).
defaultDatabase	If no index destination information is available in the input data, the index shown here is the destination of such data.
enableOnlineBucketRepair	Indicates whether to run asynchronous "online fsck" bucket repair, which runs in a process concurrently with Splunk software.
enableRealtimeSearch	Indicates if this is a real-time search. This is a global setting, not a per index setting.
frozenTimePeriodInSecs	Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years). Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.
homePath	An absolute path that contains the hot and warm buckets for the index.
homePath_expanded	An absolute filepath to the hot and warm buckets for the index.
indexThreads	Number of threads used for indexing. This is a global setting, not a per index setting.
isInternal	Indicates if this is an internal index (for example, _internal, _audit).
isReady	Indicates if an index is properly initialized.
lastInitTime	Last time the index processor was successfully initialized.

Name	Description
	This is a global setting, not a per index setting.
maxBloomBackfillBucketAge	If a bucket (warm or cold) is older than this, Splunk software does not create (or re-create) its bloom filter.
maxConcurrentOptimizes	The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
maxDataSize	The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended). Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" is typically one that gets over 10GB of data per day. • "auto" sets the size to 750MB. • "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems. Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. *Note:* The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.
maxHotBuckets	Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.
maxHotIdleSecs	Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time). If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.
maxHotSpanSecs	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). *Note:* If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.
maxMemMB	The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting.
maxMetaEntries	Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).

Name	Description
	If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.
maxTime	ISO8601 timestamp of the newest event time in the index.
maxTimeUnreplicatedNoAcks	Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored. If there are any acknowledged events sharing this raw slice, this paramater does not apply. In this case, maxTimeUnreplicatedWithAcks applies. Highest legal value is 2147483647. To disable this parameter, set to 0. *Note:* this is an advanced parameter. Understand the consequences before changing.
maxTimeUnreplicatedWithAcks	Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering). *Note:* This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.
maxTotalDataSizeMB	The maximum size of an index, in MB.
maxWarmDBCount	The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.
memPoolMB	Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.
minRawFileSyncSecs	Can be either an integer (or "disable"). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying "disable" disables syncing entirely: uncompressed slices are

Name	Description
	removed as soon as compression is complete.
minStreamGroupQueueSize	Minimum size of the queue that stores events in memory before committing them to a tsidx file.
minTime	ISO8601 timestamp of the oldest event time in the index.
partialServiceMetaPeriod	Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every <integer> seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.
processTrackerServiceInterval	How often, in seconds, the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests.
quarantineFutureSecs	Events with timestamp of quarantineFutureSecs newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.
quarantinePastSecs	Events with timestamp of quarantinePastSecs older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.
rawChunkSizeBytes	Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. *Note:* rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. *Warning:* This is an advanced parameter. Only change it if instructed to do so by Splunk Support.
repFactor	Index replication control. This parameter applies to only clustering slaves. `auto` = Use the master index replication configuration value. `0` = Turn off replication for this index.
rotatePeriodInSecs	Rotation period, in seconds, that specifies how frequently to check: • If a new hot bucket needs to be created. • If there are any cold buckets that should be frozen. • If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.

Name	Description
serviceMetaPeriod	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.
suppressBannerList	List of indexes for which we suppress "index missing" warning banner messages. This is a global setting, not a per index setting.
sync	Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.
syncMeta	When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. *Note:* Do not change this parameter without the input of Splunk Support.
thawedPath	Filepath to the thawed (resurrected) databases for the index.
thawedPath_expanded	Absolute filepath to the thawed (resurrected) databases.
throttleCheckPeriod	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). *Note:* Do not change this parameter without the input of Splunk Support.
totalEventCount	Total number of events in the index.
tsidxDedupPostingsListMaxTermsLimit	This setting is valid only when `tsidxWritingLevel` is at 4 or higher. This maximum term limit sets an upper bound on the number of terms kept inside an in-memory hash table that serves to improve tsidx compression. The tsidx optimizer uses the hash table to identify terms with identical postings lists. When the first instance of a term is received, its postings list is stored. When successive terms with identical postings lists are received, the tsidx optimizer makes them refer to the first instance of the postings list rather than creating and storing term postings list duplicates. Consider increasing this limit to improve compression for large tsidx files. For example, a tsidx file created with `tsidxTargetSizeMB` over 1500MB can contain a large number of terms with identical postings lists. Reducing this limit helps conserve memory consumed by optimization processes, at the cost of reduced tsidx compression. Set this limit to 0 to disable deduplicated postings list compression. This setting cannot exceed 1,073,741,824 (2^{30}). Defaults to 8,388,608 (2^{23}).
tstatsHomePath	Location where datamodel acceleration TSIDX data for this index is stored.
warmToColdScript	Script to run when moving data from warm to cold. See input parameter description for details.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/indexes -d name=Shadow
```

XML Response

```
...
 <title>indexes</title>
 <id>https://localhost:8089/servicesNS/admin/search/data/indexes</id>
 <updated>2011-05-13T13:09:27-07:00</updated>
 <generator version="98392"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/admin/search/data/indexes/_new" rel="create"/>
 <link href="/servicesNS/admin/search/data/indexes/_reload" rel="_reload"/>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>shadow</title>
   <id>https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow</id>
   <updated>2011-05-13T13:09:27-07:00</updated>
   <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="list"/>
   <link href="/servicesNS/nobody/search/data/indexes/shadow/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="assureUTF8">0</s:key>
       <s:key name="blockSignSize">0</s:key>
       <s:key name="blockSignatureDatabase">_blocksignature</s:key>
       <s:key name="coldPath">$SPLUNK_DB/shadow/colddb</s:key>
       <s:key name="coldPath_expanded">/Applications/splunk/var/lib/splunk/shadow/colddb</s:key>
       <s:key name="coldToFrozenDir"></s:key>
       <s:key name="coldToFrozenScript"></s:key>
       <s:key name="compressRawdata">1</s:key>
       <s:key name="currentDBSizeMB">1</s:key>
       <s:key name="datatype">event</s:key>
       <s:key name="defaultDatabase">main</s:key>
       <s:key name="eai:acl">. . .</s:key>
       <s:key name="enableRealtimeSearch">1</s:key>
       <s:key name="frozenTimePeriodInSecs">188697600</s:key>
       <s:key name="homePath">$SPLUNK_DB/shadow/db</s:key>
       <s:key name="homePath_expanded">/Applications/splunk/var/lib/splunk/shadow/db</s:key>
       <s:key name="indexThreads">auto</s:key>
       <s:key name="isInternal">0</s:key>
       <s:key name="lastInitTime">1305317367.331268</s:key>
       <s:key name="maxConcurrentOptimizes">3</s:key>
       <s:key name="maxDataSize">auto</s:key>
       <s:key name="maxHotBuckets">3</s:key>
       <s:key name="maxHotIdleSecs">0</s:key>
       <s:key name="maxHotSpanSecs">7776000</s:key>
       <s:key name="maxMemMB">5</s:key>
       <s:key name="maxMetaEntries">1000000</s:key>
       <s:key name="maxTime"></s:key>
       <s:key name="maxTotalDataSizeMB">500000</s:key>
       <s:key name="maxWarmDBCount">300</s:key>
       <s:key name="memPoolMB">auto</s:key>
       <s:key name="minRawFileSyncSecs">disable</s:key>
       <s:key name="minTime"></s:key>
       <s:key name="partialServiceMetaPeriod">0</s:key>
       <s:key name="quarantineFutureSecs">2592000</s:key>
```

```
      <s:key name="quarantinePastSecs">77760000</s:key>
      <s:key name="rawChunkSizeBytes">131072</s:key>
      <s:key name="rotatePeriodInSecs">60</s:key>
      <s:key name="serviceMetaPeriod">25</s:key>
      <s:key name="suppressBannerList"></s:key>
      <s:key name="sync">0</s:key>
      <s:key name="syncMeta">1</s:key>
      <s:key name="thawedPath">$SPLUNK_DB/shadow/thaweddb</s:key>
      <s:key name="thawedPath_expanded">/Applications/splunk/var/lib/splunk/shadow/thaweddb</s:key>
      <s:key name="throttleCheckPeriod">15</s:key>
      <s:key name="totalEventCount">0</s:key>
    </s:dict>
  </content>
</entry>
```

data/indexes/{name}

`https://<host>:<mPort>/services/data/indexes/{name}`

Access, update, or delete the `{name}` index.

DELETE

Removes the `{name}` index and the data contained in it.

Usage details

Before executing this operation, look through all `inputs.conf` files (on the indexer and on any forwarders sending data to the indexer) and make sure that none of the stanzas are directing data to the index that you plan to delete.

For example, if you want to delete an index called `nogood`, make sure the attribute/value pair `index=nogood` does not appear in any input stanzas. Once the index is deleted, Splunk software discards any data sent to that index.

The method returns HTTP status code`409` if the `{name}` index was disabled but Splunk Enterprise was not restarted. Restart Splunk Enterprise and try again.

For information on deleting indexes and deleting data from indexes, refer to Remove indexes and indexed data in *Managing Indexers and Clusters of Indexers*.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/services/data/indexes/shadow
```

XML Response

```
.
.
.
  <title>indexes</title>
 <id>https://localhost:8089/services/data/indexes</id>
 <updated>2012-08-02T11:10:16-07:00</updated>
 <generator build="131547" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/indexes/_new" rel="create"/>
 <link href="/services/data/indexes/_reload" rel="_reload"/>
    ... opensearch elements elided ...
 <s:messages/>
```

GET

Access information about the `{name}` index.

Request parameters

Name	Type	Default	Description
summarize	Boolean	`false`	[Optional] Response type: `true` = Summarized response, omitting some index details, providing a faster response. `false` = full response.

Returned values

Name	Description
assureUTF8	Indicates whether all data retreived from the index is proper UTF8. If enabled (set to True), degrades indexing performance. This is a global setting, not a per index setting.
blockSignSize	Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.
blockSignatureDatabase	The index that stores block signatures of events. This is a global setting, not a per index setting.
bloomfilterTotalSizeKB	Total size of all bloom filter files, in KB.
coldPath	Filepath to the cold databases for the index.
coldPath_expanded	Absoute filepath to the cold databases.
coldToFrozenDir	Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.

Name	Description
	Bucket freezing policy is as follows: • New style buckets (4.2 and on): removes all files but the rawdata To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory • Old style buckets (Pre-4.2): gzip all the .data and .tsidx files To thaw, unzip the zipped files and move the bucket into the thawed directory If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.
coldToFrozenScript	Path to the archiving script. See the POST parameter description for details.
compressRawdata	This value is ignored. splunkd process always compresses raw data.
currentDBSizeMB	Total size, in MB, of data stored in the index. The total incudes data in the home, cold and thawed paths.
defaultDatabase	If no index destination information is available in the input data, the index shown here is the destination of such data.
disabled	Indicates if the index is disabled.
enableRealtimeSearch	Indicates if this is a real-time search. This is a global setting, not a per index setting.
frozenTimePeriodInSecs	Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years). Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.
homePath	An absolute path that contains the hot and warm buckets for the index.
homePath_expanded	An absolute filepath to the hot and warm buckets for the index.
indexThreads	Number of threads used for indexing. This is a global setting, not a per index setting.
isInternal	Indicates if this is an internal index (for example, _internal, _audit).
lastInitTime	Last time the index processor was successfully initialized. This is a global setting, not a per index setting.
maxConcurrentOptimizes	The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
maxDataSize	The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended). Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high

Name	Description
	volume index" is typically one that gets over 10GB of data per day. • "auto" sets the size to 750MB. • "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems. Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. *Note:* The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.
maxHotBuckets	Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.
maxHotIdleSecs	Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time). If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.
maxHotSpanSecs	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). *Note:* If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.
maxMemMB	The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting.
maxMetaEntries	Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.
maxRunningProcessGroups	Maximum number of processes that the indexer fires off at a time. This is a global setting, not a per index setting.

Name	Description
maxTime	UNIX timestamp of the newest event time in the index.
maxTotalDataSizeMB	The maximum size of an index, in MB.
maxWarmDBCount	Maximum number of warm buckets.
memPoolMB	Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.
minRawFileSyncSecs	Can be either an integer (or "disable"). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying "disable" disables syncing entirely: uncompressed slices are removed as soon as compression is complete.
minTime	UNIX timestamp of the oldest event time in the index.
numBloomfilters	The number of bloom filters created for this index.
numHotBuckets	The number of hot buckets created for this index.
numWarmBuckets	The number of warm buckets created for this index.
partialServiceMetaPeriod	Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every <integer> seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.
quarantineFutureSecs	Events with timestamp of `quarantineFutureSecs` newer than "now" that are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.
quarantinePastSecs	Events with timestamp of quarantinePastSecs older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.

Name	Description
rawChunkSizeBytes	Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. *Note:* rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. *Warning:* This is an advanced parameter. Only change it if instructed to do so by Splunk Support.
rotatePeriodInSecs	Rotation period, in seconds, that specifies how frequently to check: • If a new hot bucket needs to be created. • If there are any cold buckets that should be frozen. • If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.
serviceMetaPeriod	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.
summarize	If true, leaves out certain index details, which provides a faster response.
suppressBannerList	List of indexes for which we suppress "index missing" warning banner messages. This is a global setting, not a per index setting.
sync	Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.
syncMeta	When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. *Note:* Do not change this parameter without the input of Splunk Support.
thawedPath	An absolute path that contains the thawed (resurrected) databases for the index.
thawedPath_expanded	Absolute filepath to the thawed (resurrected) databases.
throttleCheckPeriod	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). *Note:* Do not change this parameter without the input of Splunk Support.
totalEventCount	Total number of events in the index.
tsidxDedupPostingsListMaxTermsLimit	This setting is valid only when `tsidxWritingLevel` is at 4 or higher. This maximum term limit sets an upper bound on the number of terms kept inside an in-memory hash table that serves to improve tsidx compression. The tsidx optimizer uses the hash table to identify terms with identical postings lists. When the first instance of a term is received, its postings list is stored. When successive terms with identical postings lists are received, the tsidx optimizer makes them refer to the first instance of the postings list rather than creating and storing term postings list duplicates. Consider increasing this limit to improve compression for large tsidx files. For example, a tsidx file created with `tsidxTargetSizeMB` over 1500MB can contain a

Name	Description
	large number of terms with identical postings lists. Reducing this limit helps conserve memory consumed by optimization processes, at the cost of reduced tsidx compression. Set this limit to 0 to disable deduplicated postings list compression. This setting cannot exceed 1,073,741,824 (2^{30}). Defaults to 8,388,608 (2^{23}).

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow
```

XML Response

```
...
 <title>indexes</title>
 <id>https://localhost:8089/servicesNS/nobody/search/data/indexes</id>
 <updated>2011-08-01T12:25:34-07:00</updated>
 <generator version="105103"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/search/data/indexes/_new" rel="create"/>
 <link href="/servicesNS/nobody/search/data/indexes/_reload" rel="_reload"/>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>shadow</title>
   <id>https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow</id>
   <updated>2011-08-01T11:47:55-07:00</updated>
   <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="list"/>
   <link href="/servicesNS/nobody/search/data/indexes/shadow/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="edit"/>
   <link href="/servicesNS/nobody/search/data/indexes/shadow/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="assureUTF8">0</s:key>
       <s:key name="blockSignSize">0</s:key>
       <s:key name="blockSignatureDatabase">_blocksignature</s:key>
       <s:key name="bloomfilterTotalSizeKB">0</s:key>
       <s:key name="coldPath">$SPLUNK_DB/shadow/colddb</s:key>
       <s:key name="coldPath_expanded">/home/amrit/bin/splunk-current/var/lib/splunk/shadow/colddb</s:key>
       <s:key name="coldToFrozenDir"/>
       <s:key name="coldToFrozenScript"/>
       <s:key name="compressRawdata">1</s:key>
       <s:key name="currentDBSizeMB">1</s:key>
       <s:key name="defaultDatabase">main</s:key>
       <s:key name="disabled">0</s:key>
          ...eai:acl element elided ...
       <s:key name="eai:attributes">
         <s:dict>
    <s:key name="optionalFields">
      <s:list>
        <s:item>assureUTF8</s:item>
        <s:item>blockSignSize</s:item>
        <s:item>coldToFrozenDir</s:item>
        <s:item>coldToFrozenScript</s:item>
        <s:item>compressRawdata</s:item>
        <s:item>frozenTimePeriodInSecs</s:item>
        <s:item>maxConcurrentOptimizes</s:item>
        <s:item>maxDataSize</s:item>
        <s:item>maxHotBuckets</s:item>
        <s:item>maxHotIdleSecs</s:item>
        <s:item>maxHotSpanSecs</s:item>
        <s:item>maxMemMB</s:item>
        <s:item>maxMetaEntries</s:item>
        <s:item>maxRunningProcessGroups</s:item>
        <s:item>maxTotalDataSizeMB</s:item>
        <s:item>maxWarmDBCount</s:item>
        <s:item>minRawFileSyncSecs</s:item>
        <s:item>partialServiceMetaPeriod</s:item>
        <s:item>quarantineFutureSecs</s:item>
        <s:item>quarantinePastSecs</s:item>
        <s:item>rawChunkSizeBytes</s:item>
        <s:item>rotatePeriodInSecs</s:item>
        <s:item>serviceMetaPeriod</s:item>
        <s:item>suppressBannerList</s:item>
        <s:item>syncMeta</s:item>
        <s:item>throttleCheckPeriod</s:item>
      </s:list>
    </s:key>
    <s:key name="requiredFields">
      <s:list/>
    </s:key>
    <s:key name="wildcardFields">
      <s:list/>
    </s:key>
  </s:dict>
</s:key>
<s:key name="enableRealtimeSearch">1</s:key>
<s:key name="frozenTimePeriodInSecs">188697600</s:key>
<s:key name="homePath">$SPLUNK_DB/shadow/db</s:key>
<s:key name="homePath_expanded">/home/amrit/bin/splunk-current/var/lib/splunk/shadow/db</s:key>
<s:key name="indexThreads">auto</s:key>
<s:key name="isInternal">0</s:key>
<s:key name="lastInitTime">1312226552.102920</s:key>
<s:key name="maxConcurrentOptimizes">3</s:key>
<s:key name="maxDataSize">auto</s:key>
<s:key name="maxHotBuckets">3</s:key>
<s:key name="maxHotIdleSecs">0</s:key>
<s:key name="maxHotSpanSecs">7776000</s:key>
<s:key name="maxMemMB">5</s:key>
<s:key name="maxMetaEntries">1000000</s:key>
<s:key name="maxRunningProcessGroups">20</s:key>
<s:key name="maxTime"/>
<s:key name="maxTotalDataSizeMB">500000</s:key>
<s:key name="maxWarmDBCount">300</s:key>
<s:key name="memPoolMB">auto</s:key>
<s:key name="minRawFileSyncSecs">disable</s:key>
<s:key name="minTime"/>
<s:key name="numBloomfilters">0</s:key>
<s:key name="numHotBuckets">0</s:key>
<s:key name="numWarmBuckets">0</s:key>
```

```
        <s:key name="partialServiceMetaPeriod">0</s:key>
        <s:key name="quarantineFutureSecs">2592000</s:key>
        <s:key name="quarantinePastSecs">77760000</s:key>
        <s:key name="rawChunkSizeBytes">131072</s:key>
        <s:key name="rotatePeriodInSecs">60</s:key>
        <s:key name="serviceMetaPeriod">25</s:key>
        <s:key name="suppressBannerList"/>
        <s:key name="sync">0</s:key>
        <s:key name="syncMeta">1</s:key>
        <s:key name="thawedPath">$SPLUNK_DB/shadow/thaweddb</s:key>
        <s:key
name="thawedPath_expanded">/home/amrit/bin/splunk-current/var/lib/splunk/shadow/thaweddb</s:key>
        <s:key name="throttleCheckPeriod">15</s:key>
        <s:key name="totalEventCount">0</s:key>
      </s:dict>
    </content>
 </entry>
```

POST

Updates the {name} index.

Request parameters

Name	Type	Default	Description
blockSignSize	Number	0	Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.
bucketRebuildMemoryHint	String	auto	Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make. **Caution:** This is an advanced parameter. Inappropriate use of this parameter causes splunkd to not start if rebuild is required. *Do not set this parameter unless instructed by Splunk Support.* Default value, `auto`, varies by the amount of physical RAM on the host • less than 2GB RAM = 67108864 (64MB) tsidx • 2GB to 8GB RAM = 134217728 (128MB) tsidx • more than 8GB RAM = 268435456 (256MB) tsidx Values other than "auto" must be 16MB-1GB. Highest legal value (of the numerical part) is 4294967295 You can specify the value using a size suffix: "16777216" or "16MB" are equivalent.
coldToFrozenDir	String		Destination path for the frozen archive. Use as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory. Bucket freezing policy is as follows:

Name	Type	Default	Description
			- New style buckets (4.2 and on): removes all files but the rawdata To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory - Old style buckets (Pre-4.2): gzip all the .data and .tsidx files To thaw, gunzip the zipped files and move the bucket into the thawed directory If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence
coldToFrozenScript	String		Path to the archiving script. If your script requires a program to run it (for example, python), specify the program followed by the path. The script must be in $SPLUNK_HOME/bin or one of its subdirectories. Splunk software ships with an example archiving script in $SPLUNK_HOME/bin called coldToFrozenExample.py. DO NOT use this example script directly. It uses a default path, and if modified in place any changes are overwritten on upgrade. It is best to copy the example script to a new file in bin and modify it for your system. Most importantly, change the default archive path to an existing directory that fits your needs. If your new script in bin/ is named myColdToFrozen.py, set this key to the following: `coldToFrozenScript = "$SPLUNK_HOME/bin/python" "$SPLUNK_HOME/bin/myColdToFrozen.py"` By default, the example script has two possible behaviors when archiving: - For buckets created from version 4.2 and on, it removes all files except for rawdata. To thaw: cd to the frozen bucket and type `splunk rebuild .`, then copy the bucket to thawed for that index. We recommend using the coldToFrozenDir parameter unless you need to perform a more advanced operation upon freezing buckets. - For older-style buckets, we simply gzip all the .tsidx files. To thaw: cd to the frozen bucket and unzip the tsidx files, then copy the bucket to thawed for that index
compressRawdata	Boolean	true	This parameter is ignored. The splunkd process always compresses raw data.
enableOnlineBucketRepair	Boolean	true	Enables asynchronous "online fsck" bucket repair, which runs concurrently with Splunk software. When enabled, you do not have to wait until buckets are repaired to start Splunk Enterprise. However, you might observe a slight performance degratation.

Name	Type	Default	Description
frozenTimePeriodInSecs	Number	188697600	Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years). Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.
maxBloomBackfillBucketAge	Number	30d	Valid values are: Integer[m|s|h|d] If a warm or cold bucket is older than the specified age, do not create or rebuild its bloomfilter. Specify 0 to never rebuild bloomfilters. For example, if a bucket is older than specified with maxBloomBackfillBucketAge, and the rebuilding of its bloomfilter started but did not finish, do not rebuild it.
maxConcurrentOptimizes	Number	6	The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
maxDataSize	Number	auto	The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended).Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" would typically be considered one that gets over 10GB of data per day. • "auto" sets the size to 750MB. • "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems. Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. *Note:* The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.
maxHotBuckets	Number	3	Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.
maxHotIdleSecs	Number	0	Maximum life, in seconds, of a hot bucket. Defaults to 0.

Name	Type	Default	Description
			If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll. A value of 0 turns off the idle check (equivalent to INFINITE idle time).
maxHotSpanSecs	Number	7776000	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). *Note:*I f you set this too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.
maxMemMB	Number	5	The amount of memory, expressed in MB, to allocate for buffering a single tsidx file into memory before flushing to disk. Defaults to 5. The default is recommended for all environments. IMPORTANT: Calculate this number carefully. Setting this number incorrectly may have adverse effects on your systems memory and/or splunkd stability/performance.
maxMetaEntries	Number	1000000	Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the `punct` field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.
maxTimeUnreplicatedNoAcks	Number	300	Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored. If there are any acknowledged events sharing this raw slice, this paramater does not apply. In this case, maxTimeUnreplicatedWithAcks applies. Highest legal value is 2147483647. To disable this parameter, set to 0. *Note:* this is an advanced parameter. Understand the consequences before changing.
maxTimeUnreplicatedWithAcks	Number	60	Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering). *Note:* This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not

Name	Type	Default	Description
			exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.
maxTotalDataSizeMB	Number	500000	The maximum size of an index (in MB). If an index grows larger than the maximum size, the oldest data is frozen.
maxWarmDBCount	Number	300	The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.
minRawFileSyncSecs	Number	disable	Specify an integer (or "disable") for this parameter. This parameter sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying "disable" disables syncing entirely: uncompressed slices are removed as soon as compression is complete. *Note:* Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed
minStreamGroupQueueSize	Number	2000	Minimum size of the queue that stores events in memory before committing them to a tsidx file. *Caution*: Do not set this value, except under advice from Splunk Support.
partialServiceMetaPeriod	Number	0	Related to serviceMetaPeriod. If set, it enables metadata sync every <integer> seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. `partialServiceMetaPeriod` specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect. By default it is turned off (zero).
processTrackerServiceInterval	Number	1	Specifies, in seconds, how often the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests. Defaults to 15. If set to 0, the indexer checks child process status every second.

Name	Type	Default	Description
			Highest legal value is 4294967295.
quarantineFutureSecs	Number	2592000	Events with timestamp of `quarantineFutureSecs` newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.
quarantinePastSecs	Number	77760000	Events with timestamp of `quarantinePastSecs` older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.
rawChunkSizeBytes	Number	131072	Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, `rawChunkSizeBytes` is set to the default value. *Note:* rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. WARNING: This is an advanced parameter. Only change it if you are instructed to do so by Splunk Support.
repFactor	String	0	Index replication control. This parameter applies to only clustering slaves. `auto` = Use the master index replication configuration value. `0` = Turn off replication for this index.
rotatePeriodInSecs	Number	60	How frequently (in seconds) to check if a new hot bucket needs to be created. Also, how frequently to check if there are any warm/cold buckets that should be rolled/frozen.
serviceMetaPeriod	Number	25	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.
syncMeta	Boolean	true	When `true`, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. **Note**: Do not change this parameter without the input of a Splunk Support.
throttleCheckPeriod	Number	15	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). **Note**: Do not change this parameter without the input of Splunk Support.
tstatsHomePath	String		

Name	Type	Default	Description
			Location to store datamodel acceleration TSIDX data for this index. Restart splunkd after changing this parameter. If specified, it must be defined in terms of a volume definition. *Caution*: Path must be writable. *Default value*: volume:_splunk_summaries/$_index_name/tstats
warmToColdScript	String		Path to a script to run when moving data from warm to cold. This attribute is supported for backwards compatibility with Splunk software versions older than 4.0. Contact Splunk support if you need help configuring this setting. *Caution*: Migrating data across filesystems is now handled natively by splunkd. If you specify a script here, the script becomes responsible for moving the event data, and Splunk-native data migration are not used.

Returned values

Name	Description
assureUTF8	Boolean value indicating wheter all data retreived from the index is proper UTF8. If enabled (set to True), degrades indexing performance Can only be set globally.
blockSignSize	Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.
blockSignatureDatabase	The index that stores block signatures of events. This is a global setting, not a per index setting.
bucketRebuildMemoryHint	Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.
coldPath	Filepath to the cold databases for the index.
coldPath_expanded	Absoute filepath to the cold databases.
coldToFrozenDir	Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk Enterprise automatically puts frozen buckets in this directory. Bucket freezing policy is as follows: • New style buckets (4.2 and on): removes all files but the rawdata To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory • Old style buckets (Pre-4.2): gzip all the .data and .tsidx files

Name	Description
	To thaw, gunzip the zipped files and move the bucket into the thawed directory If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.
coldToFrozenScript	Path to the archiving script. See the POST parameter description for details.
compressRawdata	This value is ignored. splunkd process always compresses raw data.
currentDBSizeMB	Total size, in MB, of data stored in the index. The total incudes data in the home, cold and thawed paths.
defaultDatabase	If no index destination information is available in the input data, the index shown here is the destination of such data.
enableOnlineBucketRepair	Indicates whether to run asynchronous "online fsck" bucket repair, which runs in a process concurrently with Splunk software.
enableRealtimeSearch	Indicates if this is a real-time search. This is a global setting, not a per index setting.
frozenTimePeriodInSecs	Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years). Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.
homePath	An absolute path that contains the hot and warm buckets for the index.
homePath_expanded	An absolute filepath to the hot and warm buckets for the index.
indexThreads	Number of threads used for indexing. This is a global setting, not a per index setting.
isInternal	Indicates if this is an internal index (for example, _internal, _audit).
lastInitTime	Last time the index processor was successfully initialized. This is a global setting, not a per index setting.
maxBloomBackfillBucketAge	If a bucket (warm or cold) is older than this, Splunk Enterprise does not create (or re-create) its bloom filter.
maxConcurrentOptimizes	The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
maxDataSize	The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended). Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" is typically one that gets over 10GB of data per day. • "auto" sets the size to 750MB. • "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.

Name	Description
	Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. *Note:* The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.
maxHotBuckets	Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.
maxHotIdleSecs	Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time). If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.
maxHotSpanSecs	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). *Note:* If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.
maxMemMB	The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting.
maxMetaEntries	Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.
maxTime	UNIX timestamp of the newest event time in the index.
maxTimeUnreplicatedNoAcks	Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored. If there are any acknowledged events sharing this raw slice, this paramater does not apply. In this case, maxTimeUnreplicatedWithAcks applies.

Name	Description
	Highest legal value is 2147483647. To disable this parameter, set to 0. *Note:* this is an advanced parameter. Understand the consequences before changing.
maxTimeUnreplicatedWithAcks	Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering). *Note:* This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.
maxTotalDataSizeMB	The maximum size of an index, in MB.
maxWarmDBCount	The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.
memPoolMB	Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.
minRawFileSyncSecs	Can be either an integer (or "disable"). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying "disable" disables syncing entirely: uncompressed slices are removed as soon as compression is complete.
minStreamGroupQueueSize	Minimum size of the queue that stores events in memory before committing them to a tsidx file.
minTime	UNIX timestamp of the oldest event time in the index.
partialServiceMetaPeriod	Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every <integer> seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting

Name	Description
	has no effect.
processTrackerServiceInterval	How often, in seconds, the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests.
quarantineFutureSecs	Events with timestamp of quarantineFutureSecs newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.
quarantinePastSecs	Events with timestamp of quarantinePastSecs older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.
rawChunkSizeBytes	Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. *Note:* rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. *Warning:* This is an advanced parameter. Only change it if instructed to do so by Splunk Support.
repFactor	Index replication control. This parameter applies to only clustering slaves. `auto` = Use the master index replication configuration value. `0` = Turn off replication for this index.
rotatePeriodInSecs	Rotation period, in seconds, that specifies how frequently to check: • If a new hot bucket needs to be created. • If there are any cold buckets that should be frozen. • If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.
serviceMetaPeriod	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.
suppressBannerList	List of indexes for which we suppress "index missing" warning banner messages. This is a global setting, not a per index setting.
sync	Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.
syncMeta	When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. *Note:* Do not change this parameter without the input of Splunk Support.

Name	Description
thawedPath	Filepath to the thawed (resurrected) databases for the index.
thawedPath_expanded	Absolute filepath to the thawed (resurrected) databases.
throttleCheckPeriod	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). *Note:* Do not change this parameter without the input of Splunk Support.
totalEventCount	Total number of events in the index.
tsidxDedupPostingsListMaxTermsLimit	This setting is valid only when `tsidxWritingLevel` is at 4 or higher. This maximum term limit sets an upper bound on the number of terms kept inside an in-memory hash table that serves to improve tsidx compression. The tsidx optimizer uses the hash table to identify terms with identical postings lists. When the first instance of a term is received, its postings list is stored. When successive terms with identical postings lists are received, the tsidx optimizer makes them refer to the first instance of the postings list rather than creating and storing term postings list duplicates. Consider increasing this limit to improve compression for large tsidx files. For example, a tsidx file created with `tsidxTargetSizeMB` over 1500MB can contain a large number of terms with identical postings lists. Reducing this limit helps conserve memory consumed by optimization processes, at the cost of reduced tsidx compression. Set this limit to 0 to disable deduplicated postings list compression. This setting cannot exceed 1,073,741,824 (2^{30}). Defaults to 8,388,608 (2^{23}).
tstatsHomePath	Location where datamodel acceleration TSIDX data for this index is stored.
warmToColdScript	Script to run when moving data from warm to cold. See input parameter description for details.

Example request and response

XML Request

```
curl -k -u admin:pass -d maxTotalDataSizeMB=400000
https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow
```

XML Response

```
...
<title>indexes</title>
 <id>https://localhost:8089/servicesNS/nobody/search/data/indexes</id>
 <updated>2011-05-16T12:20:06-07:00</updated>
 <generator version="98392"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/search/data/indexes/_new" rel="create"/>
 <link href="/servicesNS/nobody/search/data/indexes/_reload" rel="_reload"/>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>shadow</title>
   <id>https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow</id>
```

```
  <updated>2011-05-16T12:18:56-07:00</updated>
  <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="list"/>
  <link href="/servicesNS/nobody/search/data/indexes/shadow/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="assureUTF8">0</s:key>
      <s:key name="blockSignSize">0</s:key>
      <s:key name="blockSignatureDatabase">_blocksignature</s:key>
      <s:key name="coldPath">$SPLUNK_DB/shadow/colddb</s:key>
      <s:key name="coldPath_expanded">/Applications/splunk4.3/var/lib/splunk/shadow/colddb</s:key>
      <s:key name="coldToFrozenDir"></s:key>
      <s:key name="coldToFrozenScript"></s:key>
      <s:key name="compressRawdata">1</s:key>
      <s:key name="currentDBSizeMB">1</s:key>
      <s:key name="defaultDatabase">main</s:key>
      <s:key name="eai:acl">. . .</s:key>
      <s:key name="enableRealtimeSearch">1</s:key>
      <s:key name="frozenTimePeriodInSecs">188697600</s:key>
      <s:key name="homePath">$SPLUNK_DB/shadow/db</s:key>
      <s:key name="homePath_expanded">/Applications/splunk4.3/var/lib/splunk/shadow/db</s:key>
      <s:key name="indexThreads">auto</s:key>
      <s:key name="isInternal">0</s:key>
      <s:key name="lastInitTime">1305573611.118477</s:key>
      <s:key name="maxConcurrentOptimizes">3</s:key>
      <s:key name="maxDataSize">auto</s:key>
      <s:key name="maxHotBuckets">3</s:key>
      <s:key name="maxHotIdleSecs">0</s:key>
      <s:key name="maxHotSpanSecs">7776000</s:key>
      <s:key name="maxMemMB">5</s:key>
      <s:key name="maxMetaEntries">1000000</s:key>
      <s:key name="maxTime"></s:key>
      <s:key name="maxTotalDataSizeMB">400000</s:key>
      <s:key name="maxWarmDBCount">300</s:key>
      <s:key name="memPoolMB">auto</s:key>
      <s:key name="minRawFileSyncSecs">disable</s:key>
      <s:key name="minTime"></s:key>
      <s:key name="partialServiceMetaPeriod">0</s:key>
      <s:key name="quarantineFutureSecs">2592000</s:key>
      <s:key name="quarantinePastSecs">77760000</s:key>
      <s:key name="rawChunkSizeBytes">131072</s:key>
      <s:key name="rotatePeriodInSecs">60</s:key>
      <s:key name="serviceMetaPeriod">25</s:key>
      <s:key name="suppressBannerList"></s:key>
      <s:key name="sync">0</s:key>
      <s:key name="syncMeta">1</s:key>
      <s:key name="thawedPath">$SPLUNK_DB/shadow/thaweddb</s:key>
      <s:key name="thawedPath_expanded">/Applications/splunk4.3/var/lib/splunk/shadow/thaweddb</s:key>
      <s:key name="throttleCheckPeriod">15</s:key>
      <s:key name="totalEventCount">0</s:key>
    </s:dict>
  </content>
</entry>
```

data/indexes-extended

```
https://<host>:<mPort>/services/data/indexes-extended
```

Access index bucket-level information. There are three bucket super-directories per index.

- home
- cold
- thawed

GET

List bucket attributes for all indexes.

Usage details

The default update period is 10 minutes, as defined by the `collectionPeriodInSecs` attribute in the `$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf` file.

Note: At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Type	Default	Description
datatype	String	all	Valid values: (all | event | metric). Specifies the type of index.

Returned values

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><i>bucket_dirs</i></td><td>(If <i>total_size</i> &gt; <code>0</code>) Lists the following attributes for each index bucket super-directory (<code>home</code>, <code>cold</code>, <code>thawed</code>).
<table>
<tr><th>Attribute</th><th>Description</th><th>home</th><th>cold</th><th>thawed</th></tr>
<tr><td>bucket_count</td><td>Number of buckets.</td><td></td><td>X</td><td>X</td></tr>
<tr><td>event_count</td><td>(If <i>size</i> &gt; <code>0</code>) Number of events in this bucket super-directory.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>event_max_time</td><td>(If <i>size</i> &gt; <code>0</code>) Highest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called <i>latest time</i>.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>event_min_time</td><td>(If <i>size</i> &gt; <code>0</code>) Lowest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called <i>earliest time</i>.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>hot_bucket_count</td><td>(If <i>size</i> &gt; <code>0</code>) Number of hot buckets.</td><td>X</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Attribute</th><th>Description</th><th>home</th><th>cold</th><th>thawed</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>size</td><td>Size (fractional MB) on disk of this bucket super-directory.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>warm_bucket_count</td><td>(If *size* > `0`) Number of warm buckets.</td><td>X</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>*name*</td><td>Index name.</td></tr>
<tr><td>*total_bucket_count*</td><td>(If *total_size* > `0`) Number of index buckets.</td></tr>
<tr><td>*total_event_count*</td><td>(If *total_size* > `0`) Number of events for index, excluding `frozen` events. Approximately equal to the *event_count* sum of all buckets.</td></tr>
<tr><td>*total_raw_size*</td><td>(If *total_size* > `0`) Cumulative size (fractional MB) on disk of the `<bucket>/rawdata/` directories of all buckets in this index, excluding `frozen`.</td></tr>
<tr><td>*total_size*</td><td>Size (fractional MB) on disk of this index.</td></tr>
</table>

Example request and response

XML Request

```
curl -k -u admin:passwd https://localhost:8089/services/data/indexes-extended
```

XML Response

```
...
<title>introspection--disk-objects--indexes</title>
 <id>https://localhost:8089/services/data/indexes-extended</id>
 <updated>2014-03-31T12:41:09-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
   ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>_audit</title>
   <id>https://localhost:8089/services/data/indexes-extended/_audit</id>
   <updated>2014-03-31T12:41:09-07:00</updated>
   <link href="/services/data/indexes-extended/_audit" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/data/indexes-extended/_audit" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="bucket_dirs">
         <s:dict>
           <s:key name="cold">
             <s:dict>
               <s:key name="bucket_count">0</s:key>
               <s:key name="size">0.000</s:key>
             </s:dict>
           </s:key>
           <s:key name="home">
```

```
            <s:dict>
              <s:key name="event_count">6169</s:key>
              <s:key name="event_max_time">1395246673</s:key>
              <s:key name="event_min_time">1394732683</s:key>
              <s:key name="hot_bucket_count">1</s:key>
              <s:key name="size">1.000</s:key>
              <s:key name="warm_bucket_count">5</s:key>
            </s:dict>
          </s:key>
          <s:key name="thawed">
            <s:dict>
              <s:key name="bucket_count">0</s:key>
              <s:key name="size">0.000</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="name">_audit</s:key>
      <s:key name="total_bucket_count">6</s:key>
      <s:key name="total_event_count">18096</s:key>
      <s:key name="total_raw_size">1.000</s:key>
      <s:key name="total_size">1.000</s:key>
    </s:dict>
  </content>
</entry>
    .
    .
    .
  elided
    .
    .
    .
<entry>
  <title>summary</title>
  <id>https://localhost:8089/services/data/indexes-extended/summary</id>
  <updated>2014-03-31T12:41:09-07:00</updated>
  <link href="/services/data/indexes-extended/summary" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/indexes-extended/summary" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="name">summary</s:key>
      <s:key name="total_size">0.000</s:key>
    </s:dict>
  </content>
</entry>
```

data/indexes-extended/{name}

```
https://<host>:<mPort>/services/data/indexes-extended/{name}
```

Access bucket-level information for the `{name}` index. There are three bucket super-directories per index.

- home
- cold
- thawed

GET

Get `{name}` bucket information.

Usage details

The default update period is 10 minutes, as defined by the `collectionPeriodInSecs` attribute in the `$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf` file.

Note: At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

Request parameters

None

Returned values

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><i>bucket_dirs</i></td><td>(If <i>total_size</i> &gt; <code>0</code>) List the following attributes for each index bucket super-directory (<code>home</code>, <code>cold</code>, <code>thawed</code>) as indicated:
<table>
<tr><th>Attribute</th><th>Description</th><th>home</th><th>cold</th><th>thawed</th></tr>
<tr><td>bucket_count</td><td>Number of buckets.</td><td></td><td>X</td><td>X</td></tr>
<tr><td>event_count</td><td>(If <i>size</i> &gt; <code>0</code>) Number of events in this bucket super-directory.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>event_max_time</td><td>(If <i>size</i> &gt; <code>0</code>) Highest time value (Unix epoc seconds) of all events in this bucket super-directory, commonly called <i>latest time</i>.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>event_min_time</td><td>(If <i>size</i> &gt; <code>0</code>) Lowest time value (Unix epoc seconds) of all events in this bucket super-directory, commonly called <i>earliest time</i>.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>hot_bucket_count</td><td>(If <i>size</i> &gt; <code>0</code>) Number of hot buckets.</td><td>X</td><td></td><td></td></tr>
<tr><td>size</td><td>Size (fractional MB) on disk of this bucket super-directory.</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>warm_bucket_count</td><td>(If <i>size</i> &gt; <code>0</code>) Number of warm buckets.</td><td>X</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td><table><tr><th>Attribute</th><th>Description</th><th>home</th><th>cold</th><th>thawed</th></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td><i>name</i></td><td>Index name.</td></tr>
<tr><td><i>total_bucket_count</i></td><td>(If <i>total_size</i> > <code>0</code>) Number of index buckets.</td></tr>
<tr><td><i>total_event_count</i></td><td>(If <i>total_size</i> > <code>0</code>) Number of events for index, excluding <code>frozen</code> events. Approximately equal to the <i>event_count</i> sum of all buckets.</td></tr>
<tr><td><i>total_raw_size</i></td><td>(If <i>total_size</i> > <code>0</code>) Cumulative size (fractional MB) on disk of the <code>&lt;bucket>/rawdata/</code> directories of all buckets in this index, excluding <code>frozen</code>.</td></tr>
<tr><td><i>total_size</i></td><td>Size (fractional MB) on disk of this index.</td></tr>
</table>

Example request and response

XML Request

```
curl -k -u admin:passwd https://localhost:8089/services/data/indexes-extended/history
```

XML Response

```
...
<title>introspection--disk-objects--indexes</title>
 <id>https://localhost:8089/services/data/indexes-extended</id>
 <updated>2014-03-31T12:42:29-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
   ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>_internal</title>
   <id>https://localhost:8089/services/data/indexes-extended/_internal</id>
   <updated>2014-03-31T12:42:29-07:00</updated>
   <link href="/services/data/indexes-extended/_internal" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/data/indexes-extended/_internal" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="bucket_dirs">
         <s:dict>
           <s:key name="cold">
             <s:dict>
               <s:key name="bucket_count">0</s:key>
               <s:key name="size">0.000</s:key>
             </s:dict>
           </s:key>
           <s:key name="home">
             <s:dict>
               <s:key name="event_count">180492</s:key>
               <s:key name="event_max_time">1395246673</s:key>
               <s:key name="event_min_time">1392167582</s:key>
```

```
              <s:key name="hot_bucket_count">3</s:key>
              <s:key name="size">9.000</s:key>
              <s:key name="warm_bucket_count">6</s:key>
            </s:dict>
          </s:key>
          <s:key name="thawed">
            <s:dict>
              <s:key name="bucket_count">0</s:key>
              <s:key name="size">0.000</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="eai:attributes">
        ... elided ...
      </s:key>
      <s:key name="name">_internal</s:key>
      <s:key name="total_bucket_count">9</s:key>
      <s:key name="total_event_count">556322</s:key>
      <s:key name="total_raw_size">28.000</s:key>
      <s:key name="total_size">22.000</s:key>
    </s:dict>
  </content>
</entry>
```

data/summaries

`https://<host>:<mPort>/services/data/summaries`
Get disk usage information about all summaries in an indexer.

GET

Gets current summary disk usage information.

Usage details

By default, this information is available five minutes after starting the Splunk deployment. Adjust this availability timing in server.conf.

Request parameters

Name	Description
report_acceleration	Optional. Use `"report_acceleration=1"` to access disk usage by report acceleration summary.
data_model_acceleration	Optional. Use `"data_model_acceleration=1"` to access disk usage by data model acceleration summary.

Pagination and filtering parameters can be used with this method.

Returned values

For each summary, the following values are returned.

Name	Description
name	Summary name.
related_indexes	Lists up to 10 indexes that contribute to this summary.
related_indexes_count	Provides total count of related indexes for this summary.
search_head_guid	GUID for the search head that created the summary data.
total_bucket_count	Number of buckets for this summary.
total_size	Total disk size for this summary, in MB.
type	Summary type, either "`report_acceleration`" or "`data_model_acceleration`".

Example request and response

XML Request

```
curl -k -u username:password https://localhost:8089/services/data/summaries
```

XML Response

```
...
<title>introspection--disk-objects--summaries</title>
  <id>https://localhost:8089/services/data/summaries</id>
  <updated>2015-09-16T16:05:35-07:00</updated>
  <generator build="8a67aa2a9bd9cced535484eb781ded292ae81b7a" version="20150914"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/summaries/_acl" rel="_acl"/>
  <opensearch:totalResults>3</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>DM_launcher_mydatamodel</title>
    <id>https://localhost:8089/services/data/summaries/DM_launcher_mydatamodel</id>
    <updated>2015-09-16T16:05:35-07:00</updated>
    <link href="/services/data/summaries/DM_launcher_mydatamodel" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/summaries/DM_launcher_mydatamodel" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list/>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="name">DM_launcher_mydatamodel</s:key>
      <s:key name="related_indexes">_internal</s:key>
      <s:key name="related_indexes_count">1</s:key>
      <s:key name="search_head_guid">A6FF485E-7AA5-412D-8E03-BE3ED42BA327</s:key>
      <s:key name="total_bucket_count">13</s:key>
      <s:key name="total_size">2.000</s:key>
      <s:key name="type">data_model_acceleration</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>search_admin_NS13c34e21cf577d62</title>
  <id>https://localhost:8089/services/data/summaries/search_admin_NS13c34e21cf577d62</id>
  <updated>2015-09-16T16:05:35-07:00</updated>
  <link href="/services/data/summaries/search_admin_NS13c34e21cf577d62" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/summaries/search_admin_NS13c34e21cf577d62" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list/>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="name">search_admin_NS13c34e21cf577d62</s:key>
      <s:key name="related_indexes">_internal</s:key>
      <s:key name="related_indexes_count">1</s:key>
      <s:key name="search_head_guid">A6FF485E-7AA5-412D-8E03-BE3ED42BA327</s:key>
```

```
        <s:key name="total_bucket_count">9</s:key>
        <s:key name="total_size">2.000</s:key>
        <s:key name="type">report_acceleration</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>search_admin_NS6f37597da0cade4c</title>
    <id>https://localhost:8089/services/data/summaries/search_admin_NS6f37597da0cade4c</id>
    <updated>2015-09-16T16:05:35-07:00</updated>
    <link href="/services/data/summaries/search_admin_NS6f37597da0cade4c" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/summaries/search_admin_NS6f37597da0cade4c" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="name">search_admin_NS6f37597da0cade4c</s:key>
        <s:key name="related_indexes">_internal</s:key>
        <s:key name="related_indexes_count">1</s:key>
        <s:key name="search_head_guid">A6FF485E-7AA5-412D-8E03-BE3ED42BA327</s:key>
        <s:key name="total_bucket_count">9</s:key>
        <s:key name="total_size">4.000</s:key>
        <s:key name="type">report_acceleration</s:key>
      </s:dict>
    </content>
  </entry>
```

data/summaries/{summary_name}

`https://<host>:<mPort>/services/data/summaries/{summary_name}`
Get disk usage information about the `{name}` indexer summary.

GET

Get disk usage information for the `{name}` summary.

Request parameters

None.

Returned values

Name	Description
name	Summary name.
related_indexes	Lists up to 10 indexes that contribute to this summary.
related_indexes_count	Provides total count of related indexes for this summary.
search_head_guid	GUID for search head creating the summary data.
total_bucket_count	Number of buckets for this summary.
total_size	Total summary disk size in MB.

Example request and response

XML Request

```
curl -k -u username:password  https://localhost:8089/services/data/summaries/my_summary
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>introspection--disk-objects--summaries</title>
  <id>https://localhost:8089/services/data/summaries</id>
  <updated>2015-09-11T15:27:46-07:00</updated>
  <generator build="049b19239844e1f7e09be3d55713c1aae663e7ae" version="20150910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/summaries/_acl" rel="_acl"/>
  <opensearch:totalResults>3</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
   ... opensearch elements elided ...
 <entry>
    <title>DM_launcher_mydatamodel</title>
    <id>https://localhost:8089/services/data/summaries/DM_launcher_mydatamodel</id>
    <updated>2015-09-11T15:27:46-07:00</updated>
    <link href="/services/data/summaries/DM_launcher_mydatamodel" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/summaries/DM_launcher_mydatamodel" rel="list"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="name">DM_launcher_mydatamodel</s:key>
        <s:key name="related_indexes">_audit,_internal</s:key>
        <s:key name="related_indexes_count">2</s:key>
        <s:key name="search_head_guid">58F60B1E-F098-41F7-BFEC-FE285489E67D</s:key>
        <s:key name="total_bucket_count">88</s:key>
        <s:key name="total_size">312.000</s:key>
      </s:dict>
    </content>
  </entry>

</feed>
```

server/health/deployment

`https://<host>:<mPort>/services/server/health/deployment`

Shows the overall health of a distributed deployment. The health of the deployment can be red, yellow, or green. The overall health of the deployment is based on the health of all features reporting to it.

Authentication and Authorization

Requires the `admin` role or `list_health` capability.

GET

Get the health status of a distributed deployment.

Request parameters

None

Returned values

Name	Datatype	Description
health	String	Indicates the overall health of the deployment. Health status can be red, yellow, or green.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/health/deployment
```

XML Response

```
<title>deployment</title>
    <id>https://localhost:8089/services/server/health/deployment</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/server/health/deployment" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/health/deployment" rel="list"/>
    <link href="/services/server/health/deployment/details" rel="details"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="health">yellow</s:key>
      </s:dict>
    </content>
  </entry>
```

server/health/deployment/details

`https://<host>:<mPort>/services/server/health/deployment/details`

Shows the overall health of the distributed deployment, as well as each feature node and its respective color.

Authentication and Authorization

Requires the `admin` role or `list_health` capability.

GET

Get health status of distributed deployment features.

Request parameters

None

Returned values

Name	Datatype	Description
health	String	Indicates the color of the feature: red, yellow or green. The color of mid-level features defaults to the worst health status color of all features reporting to it.
reason	String	Descriptive string that explains the reason the indicator is non-green.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/health/deployment/details
```

XML Response

```
<title>health-report</title>
  <id>https://localhost:8089/services/server/health</id>
  <updated>2019-08-01T13:04:45-07:00</updated>
  <generator build="8a199673a7ad87ac32419af7544dfdb1e22073ed" version="20190801"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment</title>
    <id>https://localhost:8089/services/server/health/deployment</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/server/health/deployment" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/health/deployment" rel="list"/>
    <link href="/services/server/health/deployment/details" rel="details"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="features">
          <s:dict>
            <s:key name="health">yellow</s:key>
            <s:key name="num_green">0</s:key>
            <s:key name="num_red">0</s:key>
            <s:key name="num_yellow">2</s:key>
            <s:key name="splunkd">
              <s:dict>
                <s:key name="health">yellow</s:key>
                <s:key name="indexer_clustering">
                  <s:dict>
                    <s:key name="health">yellow</s:key>
                    <s:key name="num_green">0</s:key>
                    <s:key name="num_red">0</s:key>
                    <s:key name="num_yellow">2</s:key>
                    <s:key name="slave_state">
                      <s:dict>
                        <s:key name="health">yellow</s:key>
                        <s:key name="num_green">0</s:key>
```

```
                        <s:key name="num_red">0</s:key>
                        <s:key name="num_yellow">2</s:key>
                        <s:key name="slave_state">
                          <s:dict>
                            <s:key name="description">description for the indicator TODO</s:key>
                            <s:key name="health">yellow</s:key>
                            <s:key name="instances">
                              <s:dict>
                                <s:key name="51C1A657-2E66-4138-9920-597F38495B72">
                                  <s:dict>
                                    <s:key name="guid">51C1A657-2E66-4138-9920-597F38495B72</s:key>
                                    <s:key name="health">yellow</s:key>
                                    <s:key name="measured_value">0</s:key>
                                    <s:key name="name">fool02.sv.splunk.com</s:key>
                                    <s:key name="reason">CMPeer is in manual detention.</s:key>
                                    <s:key name="timestamp">1564689878.099799</s:key>
                                  </s:dict>
                                </s:key>
                                <s:key name="BCC9FA7B-23F1-4A6B-AA2F-F88273CC557F">
                                  <s:dict>
                                    <s:key name="guid">BCC9FA7B-23F1-4A6B-AA2F-F88273CC557F</s:key>
                                    <s:key name="health">yellow</s:key>
                                    <s:key name="measured_value">0</s:key>
                                    <s:key name="name">fool03.sv.splunk.com</s:key>
                                    <s:key name="reason">CMPeer is in manual detention.</s:key>
                                    <s:key name="timestamp">1564689878.086763</s:key>
                                  </s:dict>
                                </s:key>
                                <s:key name="health">yellow</s:key>
                                <s:key name="num_green">0</s:key>
                                <s:key name="num_red">0</s:key>
                                <s:key name="num_yellow">2</s:key>
                              </s:dict>
                            </s:key>
                            <s:key name="name">slave_state</s:key>
                            <s:key name="num_green">0</s:key>
                            <s:key name="num_red">0</s:key>
                            <s:key name="num_yellow">2</s:key>
                            <s:key name="path">splunkd.indexer_clustering.slave_state.slave_state</s:key>
                          </s:dict>
                        </s:key>
                      </s:dict>
                    </s:key>
                  </s:dict>
                </s:key>
                <s:key name="num_green">0</s:key>
                <s:key name="num_red">0</s:key>
                <s:key name="num_yellow">2</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="health">yellow</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

server/health/splunkd

`https://<host>:<mPort>/services/server/health/splunkd`

Shows the overall health of `splunkd`. The health of `splunkd` can be red, yellow, or green. The health of `splunkd` is based on the health of all features reporting to it.

Authentication and Authorization

Requires the `admin` role or `list_health` capability.

GET

Get the health status of `splunkd`.

Request parameters

None

Returned values

Name	Datatype	Description
health	String	Indicates the overall health of `splunkd`. Health status can be red, yellow, or green.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/health/splunkd
```

XML Response

```
<title>health-report</title>
  <id>https://10.141.65.195:41405/services/server/health</id>
  <updated>2018-04-04T21:32:40+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/health/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>splunkd</title>
    <id>https://10.141.65.195:41405/services/server/health/splunkd</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/server/health/splunkd" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/health/splunkd" rel="list"/>
    <link href="/services/server/health/splunkd/details" rel="details"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="health">red</s:key>
      </s:dict>
    </content>
  </entry>
```

server/health/splunkd/details

`https://<host>:<mPort>/services/server/health/splunkd/details`

Shows the overall health of the `splunkd` health status tree, as well as each feature node and its respective color. For unhealthy nodes (non-green), the output includes reasons, indicators, thresholds, messages, and so on.

Authentication and Authorization

Requires the `admin` role or `list_health` capability.

GET

Get health status of splunkd features.

Request parameters

None

Returned values

Name	Datatype	Description
health	String	Indicate the color of the feature: red, yellow or green. The color of midlevel features is the worst color of all the features reporting to it.
messages	String	The last 50 messages from `splunkd.log` that might relate to the feature status change. Returned only if a feature color is not green.
reasons	String	Describes the indicator(s) that caused the feature's status to change to a non-green state. Returned only if a feature color is not green.
due_to_stanza	String	Indicates the stanza name in `health.conf` where the configuration for the non-green indicator exists.
due_to_threshold	String	Indicates the threshold because of which the color of the indicator is non-green.
due_to_threshold_value	Numeric	Indicates the value of the above threshold.
indicator	String	Name of the indicator because of which the feature is non-green.
reason	String	Descriptive string that explains the reason the indicator is non-green.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/health/splunkd/details
```

XML Response

```
<title>health-report</title>
  <id>https://10.141.65.213:42270/services/server/health</id>
  <updated>2018-04-03T20:05:34+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/health/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>splunkd</title>
    <id>https://10.141.65.213:42270/services/server/health/splunkd</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/server/health/splunkd" rel="alternate"/>
    <author>
      <name>system</name>
```

```
</author>
<link href="/services/server/health/splunkd" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="features">
      <s:dict>
        <s:key name="Data Forwarding">
          <s:dict>
            <s:key name="features">
              <s:dict>
                <s:key name="Splunk-2-Splunk Forwarding">
                  <s:dict>
                    <s:key name="features">
                      <s:dict>
                        <s:key name="TCPOutAutoLB-0">
                          <s:dict>
                            <s:key name="health">green</s:key>
                          </s:dict>
                        </s:key>
                      </s:dict>
                    </s:key>
                    <s:key name="health">green</s:key>
                  </s:dict>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="health">green</s:key>
          </s:dict>
        </s:key>
        <s:key name="File Monitor Input">
          <s:dict>
            <s:key name="features">
              <s:dict>
                <s:key name="BatchReader-0">
                  <s:dict>
                    <s:key name="health">green</s:key>
                  </s:dict>
                </s:key>
```

```
                    <s:key name="TailReader-0">
                      <s:dict>
                        <s:key name="health">green</s:key>
                      </s:dict>
                    </s:key>
                  </s:dict>
                </s:key>
                <s:key name="health">green</s:key>
              </s:dict>
            </s:key>
            <s:key name="Indexer Clustering">
              <s:dict>
                <s:key name="features">
                  <s:dict>
                    <s:key name="Cluster Bundles">
                      <s:dict>
                        <s:key name="health">green</s:key>
                      </s:dict>
                    </s:key>
                    <s:key name="Data Durability">
                      <s:dict>
                        <s:key name="health">green</s:key>
                      </s:dict>
                    </s:key>
                    <s:key name="Data Searchable">
                      <s:dict>
                        <s:key name="health">green</s:key>
                      </s:dict>
                    </s:key>
                    <s:key name="Indexers">
                      <s:dict>
                        <s:key name="health">green</s:key>
                      </s:dict>
                    </s:key>
                    <s:key name="Indexing Ready">
                      <s:dict>
                        <s:key name="health">green</s:key>
                      </s:dict>
                    </s:key>
                  </s:dict>
                </s:key>
                <s:key name="health">green</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="health">green</s:key>
      </s:dict>
    </content>
  </entry>
```

server/health-config

`https://<host>:<mPort>/services/server/health-config`
Endpoint to configure the splunkd health report.

Authentication and Authorization

Requires the `admin` role or `list_health` capability.

GET

List configuration information for the splunkd health report.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:password  https://localhost:8089/services/server/health-config
```

XML Response

```
<entry>
    <title>alert_action:email</title>
    <id>https://localhost:8089/services/server/health-config/alert_action%3Aemail</id>
    <link href="/services/server/health-config/alert_action%3Aemail" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/health-config/alert_action%3Aemail" rel="list"/>
    <link href="/services/server/health-config/alert_action%3Aemail" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.cc">a@company.com, b@company.com</s:key>
        <s:key name="action.to">c@company.com</s:key>
      </s:dict>
    </content>
</entry>

<entry>
    <title>health_reporter</title>
    <id>https://localhost:8089/services/server/health-config/health_reporter</id>
    <link href="/services/server/health-config/health_reporter" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/health-config/health_reporter" rel="list"/>
    <link href="/services/server/health-config/health_reporter" rel="edit"/>
    <content type="text/xml">
      <s:dict>
              <s:key name="alert.disabled">0</s:key>
              <s:key name="alert.actions">email, webhook</s:key>
              <s:key name="alert.min_duration_sec">600</s:key>
              <s:key name="alert.suppress_period">10m</s:key>
      </s:dict>
    </content>
</entry>

<entry>
    <title>feature:batchreader</title>
    <id>https://localhost:8089/services/server/health-config/feature%3Abatchreader</id>
    <link href="/services/server/health-config/feature%3Abatchreader" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/health-config/feature%3Abatchreader" rel="list"/>
    <link href="/services/server/health-config/feature%3Abatchreader/_reload" rel="_reload"/>
    <link href="/services/server/health-config/feature%3Abatchreader" rel="edit"/>
    <content type="text/xml">
      <s:dict>
              <s:key name="alert.disabled">0</s:key>
              <s:key name="alert.min_duration_sec">600</s:key>
              <s:key name="alert:data_out_rate.min_duration_sec">1800</s:key>
              <s:key name="indicator:data_out_rate:red">2</s:key>
              <s:key name="indicator:data_out_rate:yellow">1</s:key>
              <s:key name="disabled">0</s:key>
              <s:key name="display_name">BatchReader</s:key>
      </s:dict>
    </content>
</entry>
```

server/health-config/{alert_action}

`https://<host>:<mPort>/services/server/health-config/alert_action:<action_name>`
Configure alert actions for the splunkd health report.

Authentication and Authorization

Requires the `admin` role or `edit_health` capability.

POST

Configure alert actions for the splunkd health report.

Request parameters

Name	Type	Description
alert_action:<action_name>	String	Specify the alert action name. `<action_name>` can be one of the following: `[email | PagerDuty]`
action.to	String	Primary email address to use with the email alert action.
action.cc	String	CC email address to use with the email alert action.
action.bcc	String	BCC email address to use with the email alert action.
action.integration_url_override	String	Sets the `<integration key>` value for PagerDuty alert action. For example `action.integration_url_override=78c3b6cf0a884a538410fe2812273b0b`

Name	Type	Description
disabled	Boolean	Enables/disables the alert action. Possible values are 0 and 1. A value of 1 disables the alert action.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/health-config/alert_action:email
-d action.to=admin@example.com -d action.cc=admin2@example.com -d disabled=0
```

XML Response

```
<title>health-report-config</title>
  <id>https://10.141.65.179:52000/services/server/health-config</id>
  <updated>2018-04-02T18:36:31+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/health-config/_new" rel="create"/>
  <link href="/services/server/health-config/_reload" rel="_reload"/>
  <link href="/services/server/health-config/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

server/health-config/{feature_name}

```
https://<host>:<mPort>/services/server/health-config/feature:<feature_name>
```

Edit feature- and indicator-level settings for the splunkd health report.

Authentication and Authorization

Requires the `admin` role or `edit_health` capability.

POST

Edit feature- and indicator-level settings for the splunkd health report.

Request parameters

Name	Type	Description

Name	Type	Description
alert.disabled	Boolean	Possible values are 0 or 1. A value of 1 disables alerting for this feature. If alerting is disabled in the [health_reporter] stanza, alerting for this feature is disabled, regardless of the value set here. If the value is set to 1, alerting or all indicators is disabled. Default: 0 (enabled).
alert.min_duration_sec	Number	The minimum amount of time, in seconds, that the health status color must persist before an alert triggers.
alert.threshold_color	String	The health status color that triggers an alert. Possible values are yellow and red. Default: red.
alert:<indicator_name>.disabled	Number	Possible values are 0 or 1. A value of 1 disables alerting for this indicator. Default: 0 (enabled).
alert:<indicator_name>.min_duration_sec	Number	The minimum amount of time, in seconds, that the health status color must persist before an alert triggers for this indicator.
alert:<indicator_name>.threshold_color	String	The health status color that triggers an alert for this indicator. Possible values are yellow and red. Default: red.
disable	Boolean	Disables/enables reporting the health of the feature. Use `disabled=1` to disable the feature. Use `disabled=0` to enable the feature.
distributed_disabled	Boolean	Disables/enables reporting the health of the feature in the distributed health report Use `disabled=1` to disable the feature. Use `disabled=0` to enable the feature.
feature:<feature_name>	String	Specify the feature name. `feature_name` can be any supported feature listed in $SPLUNK_HOME/etc/system/default/health.conf.
indicator:<indicator name>:<color>	Number	The indicator threshold value that triggers a health status change to the specified color for the indicator.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:password https://localhost:8089/services/server/health-config/feature:batchreader -d
disabled=1 -d alert.disabled=0 -d alert.min_duration_sec=100 -d alert:data_out_rate.disabled=1
-d alert:data_out_rate.threshold_color=yellow
```

XML Response

```
<title>health-report-config</title>
  <id>https://10.141.65.179:52000/services/server/health-config</id>
  <updated>2018-04-02T18:36:31+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/health-config/_new" rel="create"/>
  <link href="/services/server/health-config/_reload" rel="_reload"/>
  <link href="/services/server/health-config/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

server/info

```
https://<host>:<mPort>/services/server/info?output_mode=json
```

Access information about the currently running Splunk instance.

Note: This endpoint provides information on the currently running Splunk instance. Some values returned in the GET response reflect server status information. However, this endpoint is meant to provide information on the currently running instance, not the machine where the instance is running. Server status values returned by this endpoint should be considered deprecated and might not continue to be accessible from this endpoint. Use `server/sysinfo` to access server status instead. For more information, see server/sysinfo.

GET

Get Splunk instance information.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description

activeLicenseGroup	Type of Splunk software license.
	`Enterprise`
	`Forwarder`
	`Free`
	`Invalid`
	`Trial`

addOns	Names of active add-ons.
build	The build number for this Splunk instance version.
cpu_arch	The architecture type for the CPU hosting `splunkd`. The value returned in the `server/info` response should be considered deprecated. Use server/sysinfo to access this response key and value instead.
guid	Globally unique identifier for this server.
host	Server name.
host_fqdn	*host* fully-qualified domain name.
isFree	Indicates if this server is running the Splunk instance under a free license.
isTrial	Indicates if this server is using a trial license.
kv_store_status	App KV store availability.
license_labels	Labels associated with the license used on this server.
licenseKeys	License key unique for each license.

Name	Description
licenseSignature	Hash signature for the license used on this server.
licenseState	Specifies the status of the license, which can be either OK or Expired.
master_guid	Globally unique identifier for this server.
max_users	Maximum number of users on the instance.

mode	Indicates whether the server is a dedicated forwarder. Possible values are:
	`normal`
	`dedicated forwarder`

numberOfCores	Server number of processor cores. The value returned in the `server/info` response should be considered deprecated. Use server/sysinfo to access this response key and value instead.
os_build	Software build for the server *os_version*. The value returned in the `server/info` response should be considered deprecated. Use server/sysinfo to access this response key and value instead.
os_name	Server operating system. The value returned in the `server/info` response should be considered deprecated. Use server/sysinfo to access this response key and value instead.
os_version	Server operating system version. The value returned in the `server/info` response should be considered deprecated. Use server/sysinfo to access this response key and value instead.
physicalMemoryMB	Server physical memory (MB). The value returned in the `server/info` response should be considered deprecated. Use server/sysinfo to access this response key and value instead.

product_type	Splunk software product type. One of the following values.
	`enterprise`
	`hunk`
	`lite`
	`lite_free`
	`splunk`

rtsearch_enabled	Indicates if real-time search is enabled for the instance on this server.

server_roles	Zero or more of the following possible server roles.
	`indexer`
	`universal_forwarder`
	`heavyweight_forwarder`
	`lightweight_forwarder`
	`license_master`
	`license_slave`
	`cluster_master`
	`cluster_slave`
	`cluster_search_head`
	`deployment_server`
	`deployment_client`
	`search_head`
	`search_peer`
	`shc_captain`
	`shc_deployer`
	`shc_member`
	
	See also: server/roles endpoint.

serverName	Server DNS domain name.
startup_time	Server platform start time, in seconds since January 1, 1970 (UNIX epoch).
version	Displays the Splunk platform version.
versionControlEnabled	

Name	Description
	Indicates whether the View version history option is enabled on the instance. A value of `True` means that the option is enabled.

Example request and response

JSON Request

```
curl -X GET -u admin:changeme -k "https://localhost:8106/services/server/info?output_mode=json"
```

JSON Response

```
  {
    "links": {},
    "origin": "https://localhost:8106/services/server/info",
    "updated": "2024-09-09T01:52:13-07:00",
    "generator": {
        "build": "b0122e4d425e5c0d37a7278576a02b962b3505f7",
        "version": "20240906"
    },
    "entry": [
        {
            "name": "server-info",
            "id": "https://localhost:8106/services/server/info/server-info",
            "updated": "1969-12-31T16:00:00-08:00",
            "links": {
                "alternate": "/services/server/info/server-info",
                "list": "/services/server/info/server-info"
            },
            "author": "system",
            "acl": {
                "app": "",
                "can_list": true,
                "can_write": true,
                "modifiable": false,
                "owner": "system",
                "perms": {
                    "read": [
                        "*"
                    ],
                    "write": []
                },
                "removable": false,
                "sharing": "system"
            },
            "content": {
                "activeLicenseGroup": "Enterprise",
                "activeLicenseSubgroup": "Production",
                "addOns": null,
                "build": "b0122e4d425e5c0d37a7278576a02b962b3505f7",
                "conf_generation": 7,
                "cpu_arch": "x86_64",
                "eai:acl": null,
                "federated_search_enabled": true,
                "fips_mode": false,
                "guid": "D4DBAE70-1C60-48F5-9A91-7222FDB7C528",
                "health_info": "green",
                "health_version": 2653725249,
                "host": "chieftain",
                "host_fqdn": "chieftain",
                "host_resolved": "chieftain",
                "isConverged": false,
                "isForwarding": false,
                "isFree": false,
                "isTrial": false,
                "kvStoreStatus": "failed",
                "licenseKeys": [
                    "CF4AAB0EAB5E5CD3B2E200AC6562A4028DAD54C4E7EA61144A836200420B3ADB"
                ],
                "licenseSignature": "52468815a75e22dee8211e7afaa3c171",
                "licenseState": "OK",
                "license_labels": [
                    "Splunk Internal License DO NOT DISTRIBUTE"
                ],
                "manager_guid": "D4DBAE70-1C60-48F5-9A91-7222FDB7C528",
                "manager_uri": "self",
                "master_guid": "D4DBAE70-1C60-48F5-9A91-7222FDB7C528",
                "master_uri": "self",
                "max_users": 4294967295,
                "mode": "normal",
                "numberOfCores": 50,
                "numberOfVirtualCores": 50,
                "os_build": "#35-Ubuntu SMP Thu May 7 20:20:34 UTC 2020",
                "os_name": "Linux",
                "os_name_extended": "Linux",
                "os_version": "5.4.0-31-generic",
                "physicalMemoryMB": 35840,
                "product_type": "enterprise",
                "rtsearch_enabled": true,
                "serverName": "chieftain",
                "server_roles": [
                    "indexer",
                    "license_master",
                    "license_manager"
                ],
                "shutting_down": "0",
                "startup_time": 1725871367,
                "staticAssetId": "F5B763C878861D48BD7E909BF8BFCD565B8DAC50BE0F0EE09FFF9685D2505F04",
                "version": "20240906",
                "versionControlEnabled": true
            }
        }
    ],
    "paging": {
        "total": 1,
        "perPage": 30,
        "offset": 0
    },
    "messages": []
}
```

server/introspection

```
https://<host>:<mPort>/services/server/introspection
```

Access system introspection artifacts.

See also the following associated endpoints.

- server/introspection/indexer
- server/introspection/kvstore

GET

List introspection resources.

Request parameters
None

Returned values
The endpoint returns a list of introspection artifacts.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/introspection
```

XML Response

```
...
<title></title>
 <id>https://localhost:8089/services/server/introspection</id>
 <updated>2014-08-04T11:40:23-07:00</updated>
 <generator build="221120" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 <s:messages/>
 <entry>
   <title>indexer</title>
   <id>https://localhost:8089/services/server/introspection/indexer</id>
   <updated>2014-08-04T11:40:23-07:00</updated>
   <link href="/services/server/introspection/indexer" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/introspection/indexer" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
```

```
</entry>
<entry>
  <title>kvstore</title>
  <id>https://localhost:8089/services/server/introspection/kvstore</id>
  <updated>2014-08-04T11:40:23-07:00</updated>
  <link href="/services/server/introspection/kvstore" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/kvstore" rel="list"/>
  <link href="/services/server/introspection/kvstore/_reload" rel="_reload"/>
  <content type="text/xml">
    <s:dict/>
  </content>
</entry>
<entry>
  <title>pipelines</title>
  <id>https://localhost:8089/services/server/introspection/pipelines</id>
  <updated>2014-08-04T11:40:23-07:00</updated>
  <link href="/services/server/introspection/pipelines" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/pipelines" rel="list"/>
  <content type="text/xml">
    <s:dict/>
  </content>
</entry>
<entry>
  <title>processors</title>
  <id>https://localhost:8089/services/server/introspection/processors</id>
  <updated>2014-08-04T11:40:23-07:00</updated>
  <link href="/services/server/introspection/processors" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/processors" rel="list"/>
  <content type="text/xml">
    <s:dict/>
  </content>
</entry>
<entry>
  <title>queues</title>
  <id>https://localhost:8089/services/server/introspection/queues</id>
  <updated>2014-08-04T11:40:23-07:00</updated>
  <link href="/services/server/introspection/queues" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/queues" rel="list"/>
  <content type="text/xml">
    <s:dict/>
  </content>
</entry>
```

server/introspection/indexer

`https://<host>:<mPort>/services/server/introspection/indexer`
Access the current indexer status.

See also server/introspection.

GET

Get indexer status information.

Request parameters
None

Returned values

Name	Description
average_KBps	Average indexer throughput (kbps).
reason	Status explanation. For a normal status, returns . . The following examples show possible abnormal status reasons. `"idx=<indexerName> Throttling indexer, too many tsidx files in bucket=<bucketName>. Is splunk-optimize working? If not, low disk space may be the cause." "You are low in disk space on partition <partitionName>. Indexing is paused. Will resume when free disk space rises above <minFreeMB>."`
status	Current indexer status. One of the following values. • `normal` • `throttled` • `stopped`

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/indexer
```

XML Response

```
...
 <title>introspection-indexer</title>
 <id>https://localhost:8089/services/server/introspection/indexer</id>
 <updated>2014-08-04T11:43:04-07:00</updated>
 <generator build="221120" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
```

```
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>indexer</title>
  <id>https://localhost:8089/services/server/introspection/indexer/indexer</id>
  <updated>2014-08-04T11:43:04-07:00</updated>
  <link href="/services/server/introspection/indexer/indexer" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/indexer/indexer" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="average_KBps">0.517667</s:key>
      <s:key name="eai:acl">... elided ...</s:key>
      <s:key name="reason">.</s:key>
      <s:key name="status">normal</s:key>
    </s:dict>
  </content>
</entry>
```

server/introspection/kvstore

```
https://<host>:<mPort>/services/server/introspection/kvstore
```

Access app KV store resources.

See also server/introspection.

GET

List app KV store resources.

Request parameters
None

Returned values
Lists the following app `/server/introspection/kvstore` resources.

- /collectionstats
- /replicasetstats
- /serverstatus

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore
```

XML Response

```
...
 <title></title>
 <id>https://localhost:8089/services/server/introspection/kvstore</id>
 <updated>2014-08-20T14:06:12-07:00</updated>
 <generator build="221120" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 <s:messages/>
 <entry>
   <title>collectionstats</title>
   <id>https://localhost:8089/services/server/introspection/kvstore/collectionstats</id>
   <updated>2014-08-20T14:06:12-07:00</updated>
   <link href="/services/server/introspection/kvstore/collectionstats" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/introspection/kvstore/collectionstats" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
 <entry>
   <title>replicasetstats</title>
   <id>https://localhost:8089/services/server/introspection/kvstore/replicasetstats</id>
   <updated>2014-08-20T14:06:12-07:00</updated>
   <link href="/services/server/introspection/kvstore/replicasetstats" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/introspection/kvstore/replicasetstats" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
 <entry>
   <title>serverstatus</title>
   <id>https://localhost:8089/services/server/introspection/kvstore/serverstatus</id>
   <updated>2014-08-20T14:06:12-07:00</updated>
   <link href="/services/server/introspection/kvstore/serverstatus" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/introspection/kvstore/serverstatus" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
```

server/introspection/kvstore/collectionstats

`https://<host>:<mPort>/services/server/introspection/kvstore/collectionstats`

Get storage statistics for a collection.

See also the following associated endpoints.

- server/introspection
- /replicasetstats
- /serverstatus

GET

Get collection storage statistics.

Request parameters

None

Returned values

Name	Description
data	Returns the following JSON document. • `count` - Number of collection documents or objects. • `indexSizes` - Key and size of every index on the collection. • `lastExtentSize` - Size of last allocated extent. • `nindexes` - Number of indexes on the collection. • `ns` - Current collection namespace. • `numExtents` - Number of contiguously allocated data file regions. • `paddingFactor` - Amount of space added to each document. • `size` - Collection records total size. • `storageSize`- Collection document storage allocation. • `systemFlags` - Collection flags that reflect internal server options. • `totalIndexSize` - Size of all indexes. • `userFlags` - Collection flags set by user. **Note:** Sizes are returned in MBs. For more information, see Performance Metrics.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore/collectionstats
```

XML Response

```
<title>kvstore-collectionstats</title>
<id>https://localhost:8089/services/server/introspection/kvstore/collectionstats</id>
<updated>2014-08-20T14:31:42-07:00</updated> <generator build="226873" version="6.2"/> <author>
 <name>Splunk</name>
</author>
... opensearch nodes elided ...
 <title>collectionStats</title>
 <id>https://localhost:8089/services/server/introspection/kvstore/collectionstats/collectionStats</id>
 <updated>2014-08-20T14:31:42-07:00</updated>
 <link href="/services/server/introspection/kvstore/collectionstats/collectionStats" rel="alternate"/>
 <author>
   <name>system</name>
 </author>
 <link href="/services/server/introspection/kvstore/collectionstats/collectionStats" rel="list"/>
 <content type="text/xml">
   <s:dict>
     <s:key name="data">
       <s:list>
         <s:item>
         {"ns":"search.kvstoredemo",
          "count":0,
          "size":0,
          "storageSize":8192,
          "numExtents":1,
          "nindexes":2,
          "lastExtentSize":8192,
          "paddingFactor":1,
          "systemFlags":1,
          "userFlags":1,
          "totalIndexSize":16352,
          "indexSizes":{"_id_":8176,"_UserAndKeyUniqueIndex":8176},
          "ok":1}
         </s:item>
       </s:list>
     </s:key>
     <s:key name="eai:acl"> ... elided ...</s:key>
   </s:dict>
 </content>
</entry>
```

server/introspection/kvstore/replicasetstats

`https://<host>:<mPort>/services/server/introspection/kvstore/replicasetstats`

Get the status of the replica set from the point of view of the current server.

See also the following associated endpoints.

- server/introspection
- /collectionstats
- /serverstatus

GET

Get the status of the replica set from the point of view of the current server.

Request parameters
None

Returned values

Name	Description

- `set` - Replicate Set Name set in the `server.conf` file.
- `date` - Current time in ISO format.
- `myState` - Startup process, basic operations, and potential error states:
    - `0 STARTUP` Initial member state. Cannot vote.
    - `1 PRIMARY` Only member that can accept write operations. Can vote.
    - `2 SECONDARY` Data store replication member. Can vote.
    - `3 RECOVERING` Members perform startup self-checks, or transition from completing a rollback or resync. Can vote.
    - `4 FATAL` Unrecoverable error encountered. Cannot vote.
    - `5 STARTUP2` Forks replication and election threads before becoming a secondary. Cannot vote.
    - `6 UNKNOWN` Never connected to replica set. Cannot vote.
    - `7 ARBITER` Participate in elections, do not replicate data. Can vote.
    - `8 DOWN` Cannot be accessed by the set. Cannot vote.
    - `9 ROLLBACK` Performs rollback. Can vote.
    - `10 REMOVED` Removed from the replica set. Cannot vote.
- `members` - Descriptions of members of replica set:
    - `_id` - Member ID.
    - `name` - Server name.
    - `health` - Status: `1` = up, `0` = down.
    - `state` - Replica state (See *MyState*).
    - `stateStr` - String representation of *state*.
    - `uptime` - Online interval (seconds).
    - `optime` - Information about last operations log operation.
        - `t` - 32-bit timestamp of last operation.
        - `i` - Number of operations since the last timestamp.
    - `optimeDate` - Time of last operations log operation in ISO format.
    - `lastHeartbeat` - Transmission time of last heartbeat in ISO format.
    - `lastHeartbeatRecv` - Time last heartbeat received in ISO format.
    - `pingMs` - Round-trip packet time (msec).
    - `syncingTo` - On secondary and recovering members, hostname of member from which this instance is syncing.
- `ok` - Command return status: `1` = Success, `0` = Failure.
- `oplogInfo` - Operations log information:
    - `start` - Start time.
    - `end` - End time.
    - `collectionStats` - Collection storage statistics:
        - `ns` - Current collection namespace.
        - `count` - Number of collection documents or objects.
        - `size` - Collection records total size.
        - `avgObjSize` - Average object size in collection (bytes).
        - `storageSize` - Collection document storage allocation.
        - `numExtents` - Number of contiguously allocated data file regions.
        - `nindexes` - Number of indexes on the collection.
        - `lastExtentSize` - Size of last allocated extent.
        - `paddingFactor` - Amount of space added to each document.
        - `systemFlags` - Collection flags that reflect internal server options.
        - `userFlags` - Collection flags set by user.
        - `totalIndexSize` - Size of all indexes.
        - `indexSizes` - Key and size of every index on the collection.

  - `capped` - Capped setting: `true` = capped, `false` = not capped.
  - `max` - Max collection size.
  - `ok` - Command return status: `1` = Success, `0` = Failure.
- `sources` - Operations log sources.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore/replicasetstats
```

XML Response

```
...
<title>replicasetstats</title>
<id>https://localhost:8089/services/server/introspection/kvstore/replicasetstats/replicasetstats</id>
<updated>2014-08-20T14:31:42-07:00</updated>
<link href="/services/server/introspection/kvstore/replicasetstats/replicasetstats" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/introspection/kvstore/replicasetstats/replicasetstats" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:key name="data">
      <s:list>
        <s:item>
          {
            "replSetStats": {
              "set": "splunkrs",
              "date": 1412203576000,
              "myState": 2,
              "syncingTo": "54.xxx.xxx.xxx:8191",
              "members": [
                {
                  "_id": 2,
                  "name": "54.xxx.xxx.xxx:8191",
                  "health": 1,
                  "state": 2,
                  "stateStr": "SECONDARY",
                  "uptime": 102409,
                  "optime": {
                    "t": 1412101153,
                    "i": 1
                  },
                  "optimeDate": 1412101153000,
                  "lastHeartbeat": 1412203575000,
                  "lastHeartbeatRecv": 1412203575000,
                  "pingMs": 1,
                  "syncingTo": "54.xxx.xxx.xxx:8191"
                },
                {
                  "_id": 3,
                  "name": "54.xxx.xxx.yyy:8191",
                  "health": 1,
                  "state": 2,
                  "stateStr": "SECONDARY",
                  "uptime": 102409,
                  "optime": {
                    "t": 1412101153,
                    "i": 1
                  },
                  "optimeDate": 1412101153000,
                  "lastHeartbeat": 1412203576000,
                  "lastHeartbeatRecv": 1412203575000,
                  "pingMs": 1,
                  "syncingTo": "54.xxx.xxx.yyy:8191"
                },
                        .
                        .
                        .
                      elided
                        .
                        .
                        .
                {
                  "_id": 17,
                  "name": "54.xxx.xxx.zzz:8191",
                  "health": 1,
                  "state": 2,
                  "stateStr": "SECONDARY",
                  "uptime": 102409,
                  "optime": {
                    "t": 1412101153,
                    "i": 1
                  },
                  "optimeDate": 1412101153000,
                  "lastHeartbeat": 1412203574000,
                  "lastHeartbeatRecv": 1412203575000,
                  "pingMs": 1,
                  "syncingTo": "54.xxx.xxx.zzz:8191"
                }
              ],
              "ok": 1
            },
            "oplogInfo": {
              "start": 1412022009000,
              "end": 1412101153000,
              "collectionStats": {
                "ns": "local.oplog.rs",
                "count": 631,
                "size": 166964,
                "avgObjSize": 264,
                "storageSize": 1048580080,
                "numExtents": 3,
                "nindexes": 0,
                "lastExtentSize": 4096,
                "paddingFactor": 1,
                "systemFlags": 0,
                "userFlags": 0,
                "totalIndexSize": 0,
                "indexSizes": {},
                "capped": true,
                "max": 9223372036854775808.000000,
                "ok": 1
              },
              "sources": {}
            }
```

```
          }
        </s:item>
      </s:list>
    </s:key>
    <s:key name="eai:acl"> ... elided ...</s:key>
  </s:dict>
</content>
</entry>
```

server/introspection/kvstore/serverstatus

`https://<host>:<mPort>/services/server/introspection/kvstore/serverstatus`
Get an overview of the database process state.

Monitoring applications periodically run this command to get statistical information about the database instance.

See also the following associated endpoints.

- server/introspection
- /collectionstats
- /replicasetstats

GET

Get an overview of the database process state.

Request parameters

None

Returned values

The response data is platform-dependent.

Name	Description
data	Returns the following CDATA items. • `asserts` - Number of database assertions since the server process started, for each of the following levels/types: ♦ `regular` ♦ `warning` ♦ `msg` ♦ `user` ♦ `rollovers` • `backgroundFlushing` - Write to disk flush metrics: ♦ `flushes` - Number of times writes flushed. ♦ `total_ms` - Number of msec processes used to flush writes. ♦ `average_ms` - Relationship between `flushes` and `total_ms`, in msec. ♦ `last_ms` - Number of msec the last flush took. ♦ `last_finished` (date) - ISO time of last completed write flush operation. • `connections` - Current incoming connections status and database availability: ♦ `current` - Number of active client connections. ♦ `available` - Number of unused connections available.

Name	Description
	♦ `totalCreated` - Total number of connections created, including closed connections. • `cursors` - [DEPRECATED] Current cursor and state. Use `metrics`, instead. • `dur` - (Durability) Journaling-related operations and performance. Journaling must be enabled.: ♦ `commits` - Number of transactions written to the journal during the last group commit interval. ♦ `journaledMB` - Amount of data (MB) written to the journal during the last group commit interval. ♦ `writeToDataFilesMB` - Amount of data (MB) written from journal to data files during the last group commit interval. ♦ `compression` - Compression ratio of data written to journal: `(journaled_size_of_data / uncompressed_size_of_data)` ♦ `commitsInWriteLock` - Number of commits that occurred during a write lock. ♦ `earlyCommits` - Number of commits requested before scheduled group commit time. ♦ `timeMs`: Performance during various journaling phases. ◊ `dt` - Data collection interval (msec). ◊ `prepLogBuffer` - Time spend preparing to write to journal (msec). ◊ `writeToJournal` - Time spent writing to journal (msec). ◊ `writeToDataFiles` - Time spent writing to data files after journaling (msec). ◊ `remapPrivateView` - Time spent remapping copy-on-write memory mapped views (msec). • `extra_info` - Platform-specific information: ♦ `note` - Platform-specific information. ♦ `heap_usage_bytes` - Total heap space size used by database (bytes). Applicable to *nix systems, only. ♦ `page_faults` - Total number of page faults that require disk operations. • `globalLock` - Information about the current database lock state, historical lock status, and active clients: ♦ `totalTime` - Time since database started and `globalLock` creation (usec). ♦ `lockTime` - Time since database started that `globalLock` has been held (usec). ♦ `currentQueue`: Information about operations queued because of a lock. ◊ `total` - Total number of operations queued waiting on `readers` and `writers` locks. ◊ `readers` - Number of operations queued waiting for read lock. ◊ `writers` - Number of operations queued waiting for write lock. ♦ `activeClients`: Information about number and operation types of connected clients. ◊ `total` - Total number of `readers` and `writers` connections. ◊ `readers` - Number of connected clients performing read operations. ◊ `writers` - Number of connected clients performing write operations. • `host` - Hostname and port number. • `indexCounters` - Index usage counters: ♦ `accesses` - Number of times operations accessed indexes. ♦ `hits` - Number of times index accessed and returned from memory. ♦ `misses` - Number of attempts to access index not in memory. ♦ `resets` - Number of times index counters reset since database last started. ♦ `missRatio` - Ratio of `hits` to `misses`. • `localTime` - ISO-formatted local time. • `locks` - State and read/write use of global and database-specific locks: ♦ `timeLockedMicros` - Amount of time a lock existed, for all databases of this server instance (usec). ♦ `timeAcquiringMicros` - Amount of time operations spend waiting, for lock for all databases of this server instance (usec). ♦ `admin`: Lock use in the admin database. ◊ `timeLockedMicros` - Amount of time locks existed in the admin database context (usec). ◊ `timeAcquiringMicros` - Amount of time spent waiting to acquire a lock in the admin database context (usec). ♦ `local`: Lock use in the local database. ◊ `timeLockedMicros` - Amount of time locks existed in the local database context (usec). ◊ `timeAcquiringMicros` - Amount of time spent waiting to acquire a lock in the local database context (usec). ♦ `search.`*`<collection>`*: Locks used in each collection. ◊ `timeLockedMicros` - Amount of time locks exist in the collection context (usec). ◊ `timeAcquiringMicros` - Amount of time spent waiting to acquire a lock in the collection context (usec). • `mem` - Memory usage: System architecture and memory usage metrics. ♦ `bits` - System address architecture: `32` or `64` bit architecture. ♦ `resident` - Amount of RAM currently used by the database process (MB).

Name	Description
	♦ virtual - Amount of virtual memroy used (MB). ♦ supported: true = supports extended memory information, false = does not support extended memory information. ♦ mapped - Amount of mapped memory for database (MB). ♦ mappedWithJournal - Amount of mapped memory, including journaling memory (MB). Always twice the size of mapped. • metrics - Current instance use and state: ♦ cursor: Cursor state and use. ◊ timedOut - Total number of cursors that have timed out since the server process started. ◊ open: - Information about open cursors. · noTimeout - Number of open cursors with option set to prevent timeout after a period of inactivity. · pinned - Number of pinned open cursors. · total - Number of cursors maintained for clients, typically less than zero. ♦ document: Information about document access and modification patterns and data use. Compare these values to opcounters data, which track total number of operations. ◊ deleted - Total number of deleted documents. ◊ inserted - Total number of inserted documents. ◊ returned - Total number of documents returned by queries. ◊ updated - Total number of updated documents. ♦ getLastError: Information about getLastError use. ◊ wtime: getLastError operation counts with a specified write concern that wait for one or more members of a replica set to acknowledge the write operation. · num - getLastError operation counts with a specified write concern that wait for one or more members of a replica set to acknowledge the write operation. · totalMillis - Amount of time spent performing getLastError operations with write concern that wait for one or more members of a replica set to acknowledge the write operation (msec). ◊ wtimeouts - Number of times write concern operations timed out as a result of the wtimeout threshold to getLastError. ♦ operation: Counters for several types of update and query operations handled using special operation types. ◊ fastmod - Number of update operations that neither cause documents to grow nor require updates to the index. ◊ idhack - Number of queries that contain the _key field. ◊ scanAndOrder - Number of queries that return sorted numbers that cannot perform the sort operation using an index. ♦ queryExecutor: Data from the query execution system. ◊ scanned - Number of index items scanned during queries and query-plan evaluation. ◊ scannedObjects - Total number of documents scanned during the query. ♦ record: Data related to record allocation in the on-disk memory files. ◊ moves - Number of times documents move within the on-disk representation of the data set. Documents move as a result of operations that increase the size of the document beyond their allocated record size. ♦ repl: Metrics related to the ordered history of logical writes. ◊ apply: - Information about the application of ordered history of logical writes. · batches: Information on the ordered history of logical writes application process on secondaries members of replica sets. • num - Number of batches applied across all databases. • totalMillis - Amount of time spent applying ordered history of logical write operations (msec). · ops - Number of ordered history of logical write operations. ◊ buffer: Information to track the ordered history of logical write operations buffer. · count - Number of operations on the ordered history of logical writes buffer. · maxSizeBytes/ - Maximum size of the ordered history of logical writes buffer. · sizeBytes - Current size of the contents of the ordered history of logical writes buffer. ◊ network: Network use information for the replication process. · bytes - Amount of data read from the replication sync source (bytes). · getmores: Information about queries for additional results from the ordered history of logical write operations cursor as part of the replication process.

Name	Description
	• `num` - Number of queries for additional results from the ordered history of logical write operations, which are operations that request an additional set of operations from the replication sync source. • `totalMillis` - Amount of time to collect data from queries for additional results from the ordered history of logical write operations (msec). · `ops` - Number of operations read from the replication source. · `readersCreated` - Number of queries for additional results from the ordered history of logical write operations processes created. ◊ `preload`: Information about replication pre-fetch. · `docs`: Information about documents loaded into memory during replication pre-fetch. • `num` - Number of documents loaded during replication pre-fetch. • `totalMillis` - Amount of time spent loading documents as part of replication pre-fetch (msec). · `indexes`: Information about index items loaded into memory during replication pre-fetch. • `num` - Number of index entries loaded by members before updating documents as part of replication pre-fetch. • `totalMillis` - Amount of time spent loading index entries as part of replication pre-fetch (msec). ♦ `storage`: Freelist behavior monitoring statistics. ◊ `freelist`: Freelist bucket behavior monitoring statistics. · `search`: Freelist bucket behavior monitoring search statistics. • `bucketExhausted` - Number of times bucket fully searched, requiring advance to next bucket. • `requests` - Number of times the allocation function was called. • `scanned` - Number of freelist bucket entries examined. ♦ `ttl`: Information about resource use of the ttl index process. ◊ `deletedDocuments` - Number of documents deleted from collections with a ttl index. ◊ `passes` - Number of times background process removes documents from collections with a ttl index. • `network` - Network use and state: ♦ `bytesIn` - Amount of network traffic received by this database (bytes). ♦ `bytesOut`- Amount of network traffic sent from this database (bytes). ♦ `numRequests` - Number of distinct requests received by the server. • `ok` - Command return status: `1` = Success, `0` = Failure. • `opcounters` - Overview of database operations by type, similar to `opcountersRepl`: ♦ `insert` - Number of insert operations since instance started. ♦ `query` - Number of queries since instance started. ♦ `update` - Number of update operations since instance started. ♦ `delete` - Number of delete operations since instance started. ♦ `getmore` - Number of `getmore` operations since instance started. ♦ `command` - Number of commands issued since instance started. • `opcountersRepl` - Overview of replication operations by type, similar to `opcounters`: ♦ `insert` - Number of replicated insert operations since instance started. ♦ `query` - Number of replicated queries since instance started. ♦ `update` - Number of replicated update operations since instance started. ♦ `delete` - Number of replicated delete operations since instance started. ♦ `getmore` - Number of replicated `getmore` operations since instance started. ♦ `command` - Number of replicated commands issued since instance started. • `pid` - Process ID. • `recordStats` - Page fault statistics: ♦ `accessesNotInMemory` - Number of times memory page accessed that was not resident in memory, for all databases. ♦ `pageFaultExceptionsThrown` - Number of page fault exceptions thrown when accessing data for all databases. ♦ `admin`: Admin database page fault statistics. ◊ `accessesNotInMemory` - Number of times memory page accessed that was not resident in memory, for the admin database. ◊ `pageFaultExceptionsThrown` - Number of page fault exceptions thrown when accessing data for the admin database. ♦ `local`: Local database page fault statistics.

Name	Description
	◊ accessesNotInMemory - Number of times memory page accessed that was not resident in memory, for the local database. ◊ pageFaultExceptionsThrown - Number of page fault exceptions thrown when accessing data for the local database. ♦ search.*<collection>*: Search database page fault statistics. ◊ accessesNotInMemory - Number of times memory page accessed that was not resident in memory, for the search database. ◊ pageFaultExceptionsThrown - Number of page fault exceptions thrown when accessing data for the search database. • uptime - Amount of time database process has been active (seconds). • uptimeEstimate - Amount of time database process has been active as calculated from the internal, course-grained time keeping system (seconds). • uptimeMillis - Amount of time database process has been active (msec). • version - Version number (not used). • writeBacksQueued - Write-backs queued status: true = write-backs queued, false = write-backs not queued.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore/serverstatus
```

XML Response

```
...
 <title>serverStatus</title>
 <id>https://localhost:8089/services/server/introspection/kvstore/serverstatus/serverStatus</id>
 <updated>2014-08-20T14:26:42-07:00</updated>
 <link href="/services/server/introspection/kvstore/serverstatus/serverStatus" rel="alternate"/>
 <author>
   <name>system</name>
 </author>
 <link href="/services/server/introspection/kvstore/serverstatus/serverStatus" rel="list"/>
 <content type="text/xml">
   <s:dict>
     <s:key name="data">
       <![CDATA[{
"host":"localhost:8089", "version":"2.6.3", "pid":23009, "uptime":19049, "uptimeMillis":19049447,
"uptimeEstimate":18295, "localTime":{"$date":1408570002615}, "asserts":{ "regular":0, "warning":0, "msg":0,
"user":0, "rollovers":0}, "backgroundFlushing":{ "flushes":317, "total_ms":11523, "average_ms":36.350158,
"last_ms":0, "last_finished":{"$date":1408569973325}}, "connections":{ "current":7, "available":3269,
"totalCreated":7}, "cursors":{ "note":"deprecated, use server status metrics", "clientCursors_size":0,
"totalOpen":0, "pinned":0, "totalNoTimeout":0, "timedOut":0}, "dur":{ "commits":30, "journaledMB":0,
"writeToDataFilesMB":0, "compression":0, "commitsInWriteLock":0, "earlyCommits":0, "timeMs":{ "dt":3072,
"prepLogBuffer":0, "writeToJournal":0, "writeToDataFiles":0, "remapPrivateView":0}}, "extra_info":{
"note":"fields vary by platform", "heap_usage_bytes":67624592, "page_faults":3}, "globalLock":{
"totalTime":19049447000, "lockTime":1491098, "currentQueue":{ "total":0, "readers":0, "writers":0},
"activeClients":{ "total":0, "readers":0, "writers":0}}, "indexCounters":{ "accesses":2, "hits":2,
"misses":0, "resets":0, "missRatio":0}, "locks":{ ".":{ "timeLockedMicros":{ "R":2926340, "W":1491098},
"timeAcquiringMicros":{ "R":1458997, "W":342703}}, "admin":{ "timeLockedMicros":{ "r":103638, "w":0},
"timeAcquiringMicros":{ "r":13202, "w":0}}, "local":{ "timeLockedMicros":{ "r":426518, "w":237},
"timeAcquiringMicros":{ "r":185505, "w":12}}, "search.kvstoredemo":{ "timeLockedMicros":{ "r":2832888,
"w":292}, "timeAcquiringMicros":{ "r":1310820, "w":17}}}, "network":{ "bytesIn":1133611,
"bytesOut":11628162, "numRequests":12070}, "opcounters":{ "insert":1, "query":4760, "update":0, "delete":0,
"getmore":0, "command":8264}, "opcountersRepl":{ "insert":0, "query":0, "update":0, "delete":0, "getmore":0,
"command":0}, "recordStats":{ "accessesNotInMemory":0, "pageFaultExceptionsThrown":0, "admin":{
"accessesNotInMemory":0, "pageFaultExceptionsThrown":0}, "local":{ "accessesNotInMemory":0,
"pageFaultExceptionsThrown":0}, "search.kvstoredemo":{ "accessesNotInMemory":0,
"pageFaultExceptionsThrown":0}}, "writeBacksQueued":false, "mem":{ "bits":64, "resident":58, "virtual":325,
"supported":true, "mapped":64, "mappedWithJournal":128}, "metrics":{ "cursor":{ "timedOut":0, "open":{
"noTimeout":0, "pinned":0, "total":0}}, "document":{ "deleted":0, "inserted":1, "returned":2, "updated":0},
"getLastError":{ "wtime":{ "num":0, "totalMillis":0}, "wtimeouts":0}, "operation":{ "fastmod":0, "idhack":0,
"scanAndOrder":0}, "queryExecutor":{ "scanned":0, "scannedObjects":0}, "record":{"moves":0}, "repl":{
"apply":{ "batches":{ "num":0, "totalMillis":0}, "ops":0}, "buffer":{ "count":0, "maxSizeBytes":268435456,
"sizeBytes":0}, "network":{ "bytes":0, "getmores":{ "num":0, "totalMillis":0}, "ops":0, "readersCreated":0},
"preload":{ "docs":{ "num":0, "totalMillis":0}, "indexes":{ "num":0, "totalMillis":0}}}, "storage":{
"freelist":{ "search":{ "bucketExhausted":0, "requests":0, "scanned":0}}}, "ttl":{ "deletedDocuments":0,
"passes":317}}, "ok":1}]]>

     </s:key>
     <s:key name="eai:acl"> ... elided ... </s:key>
   </s:dict>
 </content>
</entry>
```

server/introspection/search/dispatch

`https://<host>:<mPort>/services/server/introspection/search/dispatch`

Provides vital statistics for distributed search framework, including details on search peer performance.

GET

Enumerate scheduled search details.

Request parameters

None

Returned values

Name	Description
Bundle_Directory_Reaper_Average_Time(ms)	Average time for dispatch reaper to walk search peer directory and reap obsolete bundles.
Bundle_Directory_Reaper_Max_Time(ms)	Maximum time for dispatch reaper to walk search peer directory and reap obsolete bundles.
Compute_User_Search_Quota_Average_Time(ms)	Average time for computing user search quota.
Compute_User_Search_Quota_Max_Time(ms)	Maximum time for computing user search quota.
Dispatch_Directory_Reaper_Average_Time(ms)	Average time for dispatch reaper to walk dispatch directory and reap stale artifacts.
Dispatch_Directory_Reaper_Max_Time(ms)	Maximum time for dispatch reaper to walk dispatch directory and reap stale artifacts.
Search_StartUp_Time_Average_Time(ms)	Average time for preprocessing before search startup. Counted from time search state is set to `RUNNING`.

Name	Description
	Startup time indicates that parsing is complete and the distributed search infrastructure is set up. At startup, the Splunk platform is ready to wait for responses from indexers.
Search_StartUp_Time_Max_Time(ms)	Maximum time for preprocessing before search startup. Counted from time search state is set to `RUNNING`. Startup time indicates that parsing is complete and the distributed search infrastructure is set up. At startup, the Splunk platform is ready to wait for responses from indexers.

Example request and response

XML Request

```
curl -k -u username:password https://localhost:8089/services/server/introspection/search/dispatch
```

XML Response

```
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>introspection-dispatchreaper</title>
  <id>https://localhost:8089/services/server/introspection/search/dispatch</id>
  <updated>2015-08-27T13:49:04-07:00</updated>
  <generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search/dispatch/_acl" rel="_acl"/>
  <opensearch:totalResults>4</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Bundle_Directory_Reaper</title>
    <id>https://localhost:8089/services/server/introspection/search/dispatch/Bundle_Directory_Reaper</id>
    <updated>2015-08-27T13:49:04-07:00</updated>
    <link href="/services/server/introspection/search/dispatch/Bundle_Directory_Reaper" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/dispatch/Bundle_Directory_Reaper" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Bundle_Directory_Reaper_Average_Time(ms)">1.000000</s:key>
        <s:key name="Bundle_Directory_Reaper_Max_Time(ms)">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
```

```
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>Compute_User_Search_Quota</title>
<id>https://localhost:8089/services/server/introspection/search/dispatch/Compute_User_Search_Quota</id>
   <updated>2015-08-27T13:49:04-07:00</updated>
   <link href="/services/server/introspection/search/dispatch/Compute_User_Search_Quota" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/introspection/search/dispatch/Compute_User_Search_Quota" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="Compute_User_Search_Quota_Average_Time(ms)">2.500000</s:key>
       <s:key name="Compute_User_Search_Quota_Max_Time(ms)">4</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
     </s:dict>
   </content>
```

```
</entry>
<entry>
  <title>Dispatch_Directory_Reaper</title>
  <id>https://localhost:8089/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper</id>
  <updated>2015-08-27T13:49:04-07:00</updated>
  <link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="Dispatch_Directory_Reaper_Average_Time(ms)">5.400000</s:key>
      <s:key name="Dispatch_Directory_Reaper_Max_Time(ms)">16</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>Search_StartUp_Time</title>
  <id>https://localhost:8089/services/server/introspection/search/dispatch/Search_StartUp_Time</id>
  <updated>2015-08-27T13:49:04-07:00</updated>
  <link href="/services/server/introspection/search/dispatch/Search_StartUp_Time" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/search/dispatch/Search_StartUp_Time" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="Search_StartUp_Time_Average_Time(ms)">136.750000</s:key>
      <s:key name="Search_StartUp_Time_Max_Time(ms)">185</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
```

```
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

server/introspection/search/dispatch/Bundle_Directory_Reaper

`https://<host>:<mPort>/services/server/introspection/search/dispatch/Bundle_Directory_Reaper`

Get average and maximum time for the dispatch reaper to walk the search peer directory and reap obsolete bundles.

GET

Enumerate routine distributed search method execution times for each peer.

Request parameters

None

Returned values

Name	Description
Bundle_Directory_Reaper_Average_Time(ms)	Average time for dispatch reaper to walk search peer directory and reap obsolete bundles.
Bundle_Directory_Reaper_Max_Time(ms)	Maximum time for dispatch reaper to walk search peer directory and reap obsolete bundles.

Example request and response

XML Request

```
curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Bundle_Directory_Reaper
```

XML Response

```
...
  <title>introspection-dispatchreaper</title>
  <id>https://localhost:8089/services/server/introspection/search//dispatch</id>
  <updated>2015-08-26T14:24:43-07:00</updated>
  <generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search//dispatch/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Bundle_Directory_Reaper</title>
    <id>https://localhost:8089/services/server/introspection/search//dispatch/Bundle_Directory_Reaper</id>
    <updated>2015-08-26T14:24:43-07:00</updated>
    <link href="/services/server/introspection/search//dispatch/Bundle_Directory_Reaper" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search//dispatch/Bundle_Directory_Reaper" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Bundle_Directory_Reaper_Average_Time(ms)">1.000000</s:key>
        <s:key name="Bundle_Directory_Reaper_Max_Time(ms)">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

server/introspection/search/dispatch/Compute_User_Search_Quota

`https://<host>:<mPort>/services/server/introspection/search/dispatch/Compute_User_Search_Quota`

Provides average and maximum time for computing user search quotas.

GET

Enumerate average and maximum time for user search quota computation.

Request parameters

None

Returned values

Name	Description
Compute_User_Search_Quota_Average_Time(ms)	Average time for computing user search quota.
Compute_User_Search_Quota_Max_Time(ms)	Maximum time for computing user search quota.

XML Request

```
curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Compute_User_Search_Quota
```

XML Response

```
...
<title>introspection-dispatchreaper</title>
  <id>https://localhost:8089/services/server/introspection/search/dispatch</id>
  <updated>2015-08-26T14:33:46-07:00</updated>
  <generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search/dispatch/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Compute_User_Search_Quota</title>
    <id>https://localhost:8089/services/server/introspection/search/dispatch/Compute_User_Search_Quota</id>
    <updated>2015-08-26T14:33:46-07:00</updated>
    <link href="/services/server/introspection/search/dispatch/Compute_User_Search_Quota" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/dispatch/Compute_User_Search_Quota" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Compute_User_Search_Quota_Average_Time(ms)">1.950000</s:key>
        <s:key name="Compute_User_Search_Quota_Max_Time(ms)">4</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

server/introspection/search/dispatch/Dispatch_Directory_Reaper

```
https://<host>:<mPort>/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper
```

Get average and maximum time for the dispatch reaper to walk the dispatch directory and reap stale artifacts.

GET

Show dispatch directory reaper times for reaping stale artifacts.

Request parameters
None

Returned values

Name	Description
Dispatch_Directory_Reaper_Average_Time(ms)	Average time for dispatch reaper to walk dispatch directory and reap stale artifacts.
Dispatch_Directory_Reaper_Max_Time(ms)	Maximum time for dispatch reaper to walk dispatch directory and reap stale artifacts.

Example request and response

XML Request

```
curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper
```

XML Response

```
...
  <title>introspection-dispatchreaper</title>
  <id>https://localhost:8089/services/server/introspection/search/dispatch</id>
  <updated>2015-08-26T14:34:41-07:00</updated>
  <generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search/dispatch/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Dispatch_Directory_Reaper</title>
    <id>https://localhost:8089/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper</id>
    <updated>2015-08-26T14:34:41-07:00</updated>
    <link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Dispatch_Directory_Reaper_Average_Time(ms)">4.500000</s:key>
        <s:key name="Dispatch_Directory_Reaper_Max_Time(ms)">10</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

server/introspection/search/dispatch/Search_StartUp_Time

`https://<host>:<mPort>/services/server/introspection/search/dispatch/Search_StartUp_Time`

Get average and maximum time for search preprocessing before startup.

Startup time indicates that parsing is complete and the distributed search infrastructure is set up. At startup, Splunk software is ready to wait for responses from indexers.

GET

Enumerate average and maximum time for search preprocessing before startup.

Request parameters

None

Returned values

Name	Description
Search_StartUp_Time_Average_Time(ms)	Average time for preprocessing before search startup. Counted from time search state is set to `RUNNING`.
Search_StartUp_Time_Max_Time(ms)	Maximum time for preprocessing before search startup. Counted from time search state is set to `RUNNING`.

Example request and response

XML Request

```
curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Search_StartUp_Time
```

XML Response

```
...
<title>introspection-dispatchreaper</title>
  <id>https://localhost:8089/services/server/introspection/search//dispatch</id>
  <updated>2015-08-26T14:25:14-07:00</updated>
  <generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search//dispatch/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Search_StartUp_Time</title>
    <id>https://localhost:8089/services/server/introspection/search//dispatch/Search_StartUp_Time</id>
    <updated>2015-08-26T14:25:14-07:00</updated>
    <link href="/services/server/introspection/search//dispatch/Search_StartUp_Time" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search//dispatch/Search_StartUp_Time" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Search_StartUp_Time_Average_Time(ms)">128.619048</s:key>
        <s:key name="Search_StartUp_Time_Max_Time(ms)">171</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
```

```
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

server/introspection/search/distributed

`https://<host>:<mPort>/services/server/introspection/search/distributed`
Get information about the search knowledge bundle replication, if the current instance is the search head. Provides details about maximum and average time to execute routine distributed search methods, including peer info, peer bundles list, and authentication token requests from search heads.

GET

Enumerate routine distributed search method execution times for each peer.

Usage details

The default update period is ten minutes, as defined by the `collectionPeriodInSecs` attribute in the `$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf` file. If startup occurs within the last ten minutes, counts are shown from startup to the current time.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

The following values are listed for each peer.

Name	Description
Get_Authentication_Max_Time(ms)	Maximum time for search head to get authentication from this peer.
Get_Authentication_Mean_Time(ms)	Average time for search head to get authentication from this peer.
Get_BundleList_Max_Time(ms)	Maximum time for search head to get bundle list from this peer.
Get_ServerInfo_Max_Time(ms)	Maximum time for search head to get server information back from this peer.
Get_ServerInfo_Mean_Time(ms)	Average time for search head to get server information back from this peer.

Example request and response

XML Request

```
curl -k -u username:password https://localhost:8089/services/server/introspection/search/distributed
```

XML Response

```
...
 <title>search-distributedmetrics</title>
  <id>https://localhost:8089/services/server/introspection/search/distributed</id>
  <updated>2015-08-26T14:35:48-07:00</updated>
  <generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search/distributed/_acl" rel="_acl"/>
  <opensearch:totalResults>3</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>per_searchhead_metrics</title>
    <id>https://localhost:8089/services/server/introspection/search/distributed/per_searchhead_metrics</id>
    <updated>2015-08-26T14:35:48-07:00</updated>
    <link href="/services/server/introspection/search/distributed/per_searchhead_metrics" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/distributed/per_searchhead_metrics" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">0</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
```

```
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>localhost:8089</title>
    <id>https://localhost:8089/services/server/introspection/search/distributed/peer.sv.splunk.com%3A10017<
/id>
    <updated>2015-08-26T14:35:48-07:00</updated>
    <link href="/services/server/introspection/search/distributed/peer.sv.splunk.com%3A10017"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/distributed/peer.sv.splunk.com%3A10017" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Get_Authentication_Max_Time(ms)">4</s:key>
        <s:key name="Get_Authentication_Mean_Time(ms)">3.400000</s:key>
        <s:key name="Get_BundleList_Max_Time(ms)">5</s:key>
        <s:key name="Get_BundleList_Mean_Time(ms)">3.800000</s:key>
        <s:key name="Get_ServerInfo_Max_Time(ms)">14</s:key>
        <s:key name="Get_ServerInfo_Mean_Time(ms)">9.300000</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">0</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>window_metrics</title>
    <id>https://localhost:8089/services/server/introspection/search/distributed/window_metrics</id>
    <updated>2015-08-26T14:35:48-07:00</updated>
    <link href="/services/server/introspection/search/distributed/window_metrics" rel="alternate"/>
    <author>
```

```
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/distributed/window_metrics" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="average_bytes">0.000000</s:key>
        <s:key name="average_msecs">0.000000</s:key>
        <s:key name="count">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">0</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

server/introspection/search/saved

`https://<host>:<mPort>/services/server/introspection/search/saved`
Access most recent scheduled search priority scores and score calculation adjustments.

GET

Enumerate scheduled search details.

Request parameters
None

Returned values
'*Note:* 'These response data keys are for informational purposes only. They are subject to change or removal at any time.

Name	Description
final_score	Most recent calculated priority score, based on adjustments and original score.

Name	Description
name	Scheduled search name.
orig_score	A score based on a search's originally scheduled run time.
owner	Search scope or context owner. This could be a specific user or "nobody" for a search defined in an app or system-level scope.
priority_no	Most recent calculated priority number for this search.
real_time_adj	Real-time search priority adjustment. Real-time searches default to -80000 and continuous scheduled searches default to 0. This particular value is for internal purposes only and is subject to change.
runtime_adj	Calculated value based on average search runtime.
skipped_adj	Adjustment for number of times search has been skipped and search period. 0 means the search has not been skipped.
window_adj	Adjustment for remaining time in search run window.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/introspection/search/saved
```

XML Response

```
  <title>introspection-savedsearches</title>
  <id>https://localhost:8089/services/server/introspection/search/saved</id>
  <updated>2015-06-03T16:41:21-07:00</updated>
  <generator build="6cfc0237739f" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search/saved/_acl" rel="_acl"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>admin;search;search_1</title>
    <id>https://localhost:8089/services/server/introspection/search/saved/admin%3Bsearch%3Bsearch_1</id>
    <updated>2015-06-03T16:41:21-07:00</updated>
    <link href="/services/server/introspection/search/saved/admin%3Bsearch%3Bsearch_1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/saved/admin%3Bsearch%3Bsearch_1" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
```

```
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="final_score">1433294868</s:key>
        <s:key name="name">search_1</s:key>
        <s:key name="orig_score">1433374860</s:key>
        <s:key name="owner">admin</s:key>
        <s:key name="priority_no">1</s:key>
        <s:key name="real_time_adj">-80000</s:key>
        <s:key name="runtime_adj">8</s:key>
        <s:key name="skipped_adj">0</s:key>
        <s:key name="window_adj">0</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>nobody;search;Errors in the last hour</title>
    <id>https://localhost:8089/services/server/introspection/search/saved
/nobody%3Bsearch%3BErrors%20in%20the%20last%20hour</id>
    <updated>2015-06-03T16:41:21-07:00</updated>
    <link
href="/services/server/introspection/search/saved/nobody%3Bsearch%3BErrors%20in%20the%20last%20hour"
rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/server/introspection/search/saved/nobody%3Bsearch%3BErrors%20in%20the%20last%20hour"
rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="final_score">1433294980</s:key>
        <s:key name="name">Errors in the last hour</s:key>
        <s:key name="orig_score">1433374860</s:key>
        <s:key name="owner">nobody</s:key>
        <s:key name="priority_no">2</s:key>
        <s:key name="real_time_adj">-80000</s:key>
        <s:key name="runtime_adj">1</s:key>
        <s:key name="skipped_adj">0</s:key>
        <s:key name="window_adj">119</s:key>
      </s:dict>
    </content>
  </entry>
```

server/status

`https://<host>:<mPort>/services/server/status`
List `server/status` child resources.

GET

Enumerate server/status endpoints.

Request parameters

None

Returned values

Returns `/server/status/` child endpoints.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status
```

XML Response

```
...
 <title></title>
 <id>https://localhost:8089/services/server/status</id>
 <updated>2014-03-25T13:52:59-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <s:messages/>
 <entry>
   <title>dispatch-artifacts</title>
   <id>https://localhost:8089/services/server/status/dispatch-artifacts</id>
   <updated>2014-03-25T13:52:59-07:00</updated>
   <link href="/services/server/status/dispatch-artifacts" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/dispatch-artifacts" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
 <entry>
   <title>fishbucket</title>
   <id>https://localhost:8089/services/server/status/fishbucket</id>
   <updated>2014-03-25T13:52:59-07:00</updated>
   <link href="/services/server/status/fishbucket" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/fishbucket" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
 <entry>
   <title>partitions-space</title>
   <id>https://localhost:8089/services/server/status/partitions-space</id>
   <updated>2014-03-25T13:52:59-07:00</updated>
   <link href="/services/server/status/partitions-space" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/partitions-space" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
```

server/status/dispatch-artifacts

`https://<host>:<mPort>/services/server/status/dispatch-artifacts`
Access search job information.

GET

Get information about dispatched search jobs.

Usage details

At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters

None

Returned values

Name	Description
count_realtime	Jobs active in the immediate past observation period, not including historical jobs.
count_scheduled	Jobs active in the immediate past observation period, not including real-time jobs.
count_summary	Jobs active in the immediate past observation period, not including non-summary jobs.
top_apps	Top 15 apps in the past observation period, in*app*:*count* key-value pair format.
top_named_searches	Top 15 named searches in the past observation period, in *savedSearchName*:*count* key-value pair format.
top_users	Top 15 users in the past observation period, in *username*:*count* key-value pair format, with *count* as the number of app contexts for the user.
total_count	Number of dispatched search jobs since start-up.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/dispatch-artifacts
```

XML Response

```
...
<title>introspection--disk-objects--search-dispatch-artifacts</title>
 <id>https://localhost:8089/services/server/status/dispatch-artifacts</id>
 <updated>2014-03-25T11:10:33-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>result</title>
   <id>https://localhost:8089/services/server/status/dispatch-artifacts/result</id>
   <updated>2014-03-25T11:10:33-07:00</updated>
   <link href="/services/server/status/dispatch-artifacts/result" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/dispatch-artifacts/result" rel="list"/>
   <content type="text/xml">
```

```
     <s:dict>
       <s:key name="count_realtime">0</s:key>
       <s:key name="count_scheduled">0</s:key>
       <s:key name="count_summary">0</s:key>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="top_apps"/>
       <s:key name="top_named_searches"/>
       <s:key name="top_users"/>
       <s:key name="total_count">0</s:key>
     </s:dict>
   </content>
 </entry>
```

server/status/fishbucket

`https://<host>:<mPort>/services/server/status/fishbucket`
Access information about the private BTree database.

GET

Access private BTree database information.

Usage details

At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters

None

Returned values

Name	Description
key_count	Number of file input records (keys) seen since start-up.
total_size	Total number of file input records (keys).

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/fishbucket
```

XML Response

```
...
 <title>introspection--disk-objects--fishbucket</title>
 <id>https://localhost:8089/services/server/status/fishbucket</id>
 <updated>2014-03-25T11:31:10-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>result</title>
   <id>https://localhost:8089/services/server/status/fishbucket/result</id>
   <updated>2014-03-25T11:31:10-07:00</updated>
   <link href="/services/server/status/fishbucket/result" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/fishbucket/result" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="key_count">0</s:key>
       <s:key name="total_size">0.000</s:key>
     </s:dict>
   </content>
 </entry>
```

server/status/installed-file-integrity

Check for system file irregularities.

```
https://<host>:<mPort>/services/server/status/installed-file-integrity
```

GET

Check file integrity status.

Usage details

The GET request returns cached results for an automatic check of all files installed with the currently running Splunk software version. The check compares currently installed files against the manifest file located in the `$SPLUNK_HOME` directory. Based on this comparison, the GET response shows an integrity status indicator for each installed file.

By default, this check runs at startup and results are cached when the check completes. The check takes a few minutes to run and results are available after it completes. The response indicates if initial results are not yet ready when the GET request is performed or if the check is disabled.

You can prompt a new check to run by passing in `?refresh=true` with the GET request.

To disable the file integrity check, edit the `installed_files_integrity` setting in the `limits.conf` file.

Note: Changing or removing the manifest file prevents the check from working.

Request parameters

Name	Type	Description
refresh	Boolean	Set to `true` to perform a new file integrity check. Only one such check can be performed at a time.
regex_filter	PCRE regular expression	Specify a regular expression to filter results of the check. For example, use `regex_filter=\.conf$` to filter results for configuration files.

Returned values

For each installed file, one of the following integrity status indicators is returned.

Indicator	Description
<empty>	Indicates complete file integrity. No irregularities were found.
access_failed	The `splunkd` process does not have permissions to read the file.
differs	The installed file differs from the manifest file.
missing	The installed file was not found.
read_failed	The installed file comparison failed.
other_open_failed	A failure other than failure to access or read was encountered when trying to open the file.

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/server/status/installed-file-integrity?refresh=true
```

XML Response

The following example is a portion of the response data. The full response lists all installed files and their integrity status.

```
...

<s:key name="/opt/splunktest/etc/system/README/inputs.conf.example">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/inputs.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/limits.conf.example">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/limits.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/messages.conf.example">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/props.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/savedsearches.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/server.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/user-prefs.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/web.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/bin/field_extractor.py">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/app.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/authorize.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/indexes.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/inputs.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/limits.conf">differs</s:key>
```

```
...
```

server/status/limits/search-concurrency

`https://<host>:<mPort>/services/server/status/limits/search-concurrency`

Access search concurrency metrics for a standalone Splunk Enterprise instance.

GET

Get search concurrency limits for a standalone Splunk Enterprise instance.

Request parameters

None

Returned values

Name	Description
max_auto_summary_searches	Maximum number of auto summary searches.
max_hist_scheduled_searches	Maximum number of historical scheduled searches.
max_hist_searches	Maximum number of historical searches.
max_rt_scheduled_searches	Maximum number of scheduled searches.
max_rt_searches	Maximum number of real-time searches.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/limits/search-concurrency
```

XML Response

```
...
 <title>server-status-limits-concurrency</title>
 <id>https://localhost:8089/services/server/status/limits/search-concurrency</id>
 <updated>2014-03-25T11:40:16-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>search-concurrency</title>
   <id>https://localhost:8089/services/server/status/limits/search-concurrency/search-concurrency</id>
   <updated>2014-03-25T11:40:16-07:00</updated>
```

```
  <link href="/services/server/status/limits/search-concurrency/search-concurrency" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/status/limits/search-concurrency/search-concurrency" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="max_auto_summary_searches">2</s:key>
      <s:key name="max_hist_scheduled_searches">5</s:key>
      <s:key name="max_hist_searches">10</s:key>
      <s:key name="max_rt_scheduled_searches">5</s:key>
      <s:key name="max_rt_searches">10</s:key>
    </s:dict>
  </content>
</entry>
```

server/status/partitions-space

```
https://<host>:<mPort>/services/server/status/partitions-space
```

Access disk utilization information for filesystems that have Splunk objects, such as indexes, volumes, and logs. A filesystem can span multiple physical disk partitions.

GET

Get disk utilization information.

Usage details

At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
capacity	Disk capacity (MB).

Name	Description
free	Disk free space (MB).
fs_type	File system type. Example values: • Linux: ext2, ext3, ext4, qnx4 • Solaris: ufs, zfs • Windows: ntfs, fat32 • AIX: jfs • (not OS-specific) WORM: ISO9660, UDF13346 • (not OS-specific); network-shared: SMB, CIFS, NFS • (not OS-specific) Veritas: VxFS.
mount_point	Absolute path of the directory where this partition is mounted.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/partitions-space
```

XML Response

```
...
<title>introspection--disk-objects--partitions-space</title>
 <id>https://localhost:8089/services/server/status/partitions-space</id>
 <updated>2014-03-25T11:43:39-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>0</title>
   <id>https://localhost:8089/services/server/status/partitions-space/0</id>
   <updated>2014-03-25T11:43:39-07:00</updated>
   <link href="/services/server/status/partitions-space/0" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/partitions-space/0" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="capacity">104901.000</s:key>
       <s:key name="eai:acl">
         ... elided ...
       </s:key>
       <s:key name="free">7774.000</s:key>
       <s:key name="fs_type">ntfs</s:key>
       <s:key name="mount_point">C:\</s:key>
     </s:dict>
   </content>
 </entry>
```

server/status/resource-usage

`https://<host>:<mPort>/services/server/status/resource-usage`
Get current resource (CPU, RAM, VM, I/O, file handle) utilization for entire host, and per Splunk-related processes.

GET

Get resource utilization information.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
Returns a list of `server/status/resource-usage/` endpoints.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/resource-usage
```

XML Response

```
...
<title></title>
 <id>https://localhost:8089/services/server/status/resource-usage</id>
 <updated>2014-03-25T11:53:26-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <s:messages/>
 <entry>
   <title>hostwide</title>
   <id>https://localhost:8089/services/server/status/resource-usage/hostwide</id>
   <updated>2014-03-25T11:53:26-07:00</updated>
   <link href="/services/server/status/resource-usage/hostwide" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/resource-usage/hostwide" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
 <entry>
   <title>splunk-processes</title>
   <id>https://localhost:8089/services/server/status/resource-usage/splunk-processes</id>
   <updated>2014-03-25T11:53:26-07:00</updated>
   <link href="/services/server/status/resource-usage/splunk-processes" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/status/resource-usage/splunk-processes" rel="list"/>
   <content type="text/xml">
     <s:dict/>
   </content>
 </entry>
```

server/status/resource-usage/hostwide

`https://<host>:<mPort>/services/server/status/resource-usage/hostwide`
Access host-level dynamic CPU utilization and paging information.

GET

Get host-level, dynamic CPU utilization and paging information.

Usage details

At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters

None

Returned values

Name	Description
cpu_arch	CPU architecture
cpu_count	CPU count
cpu_idle_pct	Percentage of time CPU is idle.

Name	Description
cpu_system_pct	Percentage of time CPU is running in system mode.
cpu_user_pct	Percentage of time CPU is running in user mode.
forks	Cumulative number of forked processes since OS startup.
mem	Total physical memory available (MB)
mem_used	Total physical memory used (MB). This value represents the amount of actual physical memory minus the amount of physical memory currently available. This is the amount of physical memory that can be immediately reused without having to first write its contents to disk. On Unix, *mem_used* = `total_phys_ram - (free_mem + buffer_mem + cached_mem)` On Windows, *mem_used* = `(memoryStatus.ullTotalPhys - memoryStatus.ullAvailPhys)` See GlobalMemoryStatusEx function for more information.
normalized_load_avg_1min	Normalized load average of *runnable_process_count* across all cores (cumulative_load_avg / number_of_cores). This value is not reliable for a VM guest.
os_build	Software build for the *os_version*
os_name	Operating system name
os_name_ext	Extended operating system name
os_version	Operating system version
pg_paged_out	Cumulative VM page count paged since OS startup. Not available on Windows.
pg_swapped_out	Cumulative pages swapped out since OS startup. Not available on Windows.
runnable_process_count	Number of process running or in the runnable queue. Value reported as 1 on Windows except for Vista+ and XP/Win2003 English-only operating systems.
splunk_version	Currently installed Splunk software version
swap	Amount of disk allocated to swap (fractional MB)
swap_used	Swap space currently in use (fractional MB)
virtual_cpu_count	Virtual CPU count

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/resource-usage/hostwide
```

XML Response

```
  <title>introspection--resource-usage--hostwide</title>
  <id>https://localhost:8089/services/server/status/resource-usage/hostwide</id>
  <updated>2016-09-19T12:56:56-07:00</updated>
  <generator build="bf83e168dd2e" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/status/resource-usage/hostwide/_acl" rel="_acl"/>
```

```
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>result</title>
  <id>https://localhost:8089/services/server/status/resource-usage/hostwide/result</id>
  <updated>2016-09-19T12:56:56-07:00</updated>
  <link href="/services/server/status/resource-usage/hostwide/result" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/status/resource-usage/hostwide/result" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="cpu_arch">x86_64</s:key>
      <s:key name="cpu_count">4</s:key>
      <s:key name="cpu_idle_pct">99.37</s:key>
      <s:key name="cpu_system_pct">0.25</s:key>
      <s:key name="cpu_user_pct">0.38</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list/>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="forks">16462040</s:key>
      <s:key name="instance_guid">88F85972-368E-45F8-A123-FDB14AE9701E</s:key>
      <s:key name="mem">7872.781</s:key>
      <s:key name="mem_used">929.883</s:key>
      <s:key name="normalized_load_avg_1min">0.00</s:key>
      <s:key name="os_build">#1 SMP Fri Aug 24 01:07:11 UTC 2012</s:key>
      <s:key name="os_name">Linux</s:key>
      <s:key name="os_name_ext">Linux</s:key>
      <s:key name="os_version">2.6.32-279.5.2.el6.x86_64</s:key>
      <s:key name="pg_paged_out">732923572</s:key>
      <s:key name="pg_swapped_out">0</s:key>
      <s:key name="runnable_process_count">1</s:key>
      <s:key name="splunk_version">6.5.0</s:key>
      <s:key name="swap">4031.992</s:key>
      <s:key name="swap_used">0.000</s:key>
      <s:key name="virtual_cpu_count">4</s:key>
    </s:dict>
  </content>
</entry>
```

server/status/resource-usage/iostats

```
https://<host>:<mPort>/services/server/status/resource-usage/iostats
```

Access the most recent disk I/O statistics for each disk. This endpoint is currently supported for Linux, Windows, and Solaris. By default this endpoint is updated every 60s seconds.

GET

Get disk I/O statistics.

Request parameters

None

Returned values

Name	Description
avg_service_ms	Average time requests caused the CPU to be in use, in milliseconds.
avg_total_ms	Average queue + execution time for requests to be completed, in milliseconds.
cpu_pct	Percentage of time the CPU was servicing requests.
device	Device name (e.g., as listed under /dev on UNIX).
fs_type	Mounted device file system type.
interval	Interval over which sampling occurred, in seconds.
mount_point	Mount point(s) of the underlying device.
reads_kb_ps	Total number of kb read per second.
reads_ps	Number of read requests per second.
writes_kb_ps	Total number of kb written per second.
writes_ps	Number of write requests per second.

Example request and response

XML Request

```
curl -k -u username:password https://localhost:8089/services/server/status/resource-usage/iostats
```

XML Response

```
...
<title>introspection--resource-usage--iostats</title>
```

```
<id>https://localhost:8089/services/server/status/resource-usage/iostats</id>
<updated>2015-09-11T14:10:45-04:00</updated>
<generator build="78167cb4239c44472aa42425ebc83481b2d83433" version="20150910"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/status/resource-usage/iostats/_acl" rel="_acl"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>0</title>
  <id>https://localhost:8089/services/server/status/resource-usage/iostats/0</id>
  <updated>2015-09-11T14:10:45-04:00</updated>
  <link href="/services/server/status/resource-usage/iostats/0" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/status/resource-usage/iostats/0" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="avg_service_ms">0.142</s:key>
      <s:key name="avg_total_ms">4.110</s:key>
      <s:key name="cpu_pct">0.05</s:key>
      <s:key name="device">dm-1</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list/>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="fs_type">xfs</s:key>
      <s:key name="interval">60</s:key>
      <s:key name="mount_point">/</s:key>
      <s:key name="reads_kb_ps">0.000</s:key>
      <s:key name="reads_ps">0.000</s:key>
      <s:key name="writes_kb_ps">43.050</s:key>
      <s:key name="writes_ps">3.633</s:key>
    </s:dict>
  </content>
</entry>
```

server/status/resource-usage/splunk-processes

`https://<host>:<mPort>/services/server/status/resource-usage/splunk-processes`
Access operating system resource utilization information.

GET

Get process operating system resource utilization information.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
None

Returned values

Name	Description
args	Non-search process arguments.
cpu_system_time	Cumulative time this process has spent executing in kernel (incl. system calls). Extra field.
cpu_user_time	Cumulative time this process has spent executing in user space (incl. library functions). Extra field.
elapsed	Elapsed wall time, accurate to within the collection period.
fd_used	Number of currently open files used by this process.
label	Human-readable label for the saved search.
mem_unshared_data_used	Amount of heap and stack used. Not available on Windows. Extra field.
mem_used	Current amount of resident physical memory used (MB). (Usually far less deceiving than virtual memory because operating systems can be liberal with virtual memory size but never with resident memory size.) On Windows, *mem_used* is obtained by reading the `WorkingSetSize` property returned by the `GetProcessMemoryInfo()` function (see GetProcessMemoryInfo function and PROCESS_MEMORY_COUNTERS structure).
normalized_pct_cpu	Percentage of CPU usage across all cores. `100%` is equivalent to all CPU resources on the machine.
page_faults	Number of major page faults. Extra field.
pct_cpu	Percentage of CPU usage, relative to one core. `100%` is equivalent to 1 core.
pct_memory	Percentage of physical memory used hostwide ((*mem_used*/available_host_memory) * 100).
pid	Process ID.

Name	Description
ppid	Parent process ID. Not available for all processes.
process	Process name. The `.exe` suffix is stripped on Windows operating systems.
read_mb	Amount of data read (MB), excluding cache reads.
search_head	Dispatching search head for processes running saved searches.
search_props	Search properties map of the following key value pairs. • `acceleration_id`: Acceleration ID • `app`: App name • `mode`: One of the following search modes. ♦ `historical` ♦ `historical batch` ♦ `RT` ♦ `RT indexed` • `provenance`: One of the following search sources. ♦ `cli` ♦ `rest` ♦ `ui:<App>:<View>` • `role`: Splunk Enterprise platform role. Either `head` or `peer`. • `scan_count`: Event scan count for running process. Available only in Linux systems. This property is offered experimentally and might be changed or removed in a future release. • `delta_scan_count`: Delta event scan count for running process. Available only in Linux systems. This property is offered experimentally and might be changed or removed in a future release. • `sid`: Search ID (SID). • `type`: One of the following search types. ♦ `ad-hoc` ♦ `datamodel acceleration` ♦ `other` ♦ `report acceleration` ♦ `scheduled` ♦ `summary indexing` • `user`: Splunk username who initiated the search
status	Status from the OS scheduler. Can be R (runnable or running), W (waiting), stopped, Z (zombie), or O (other). W includes voluntary sleep or blocking on I/O. O means status is knowable but does not fit into one of those categories. Not available on Windows.
t_count	Current number of threads.
written_mb	Amount of data written (MB), excluding canceled writes.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/resource-usage/splunk-processes/0
```

XML Response

```
<title>introspection--resource-usage--splunk-processes</title>
 <id>https://localhost:8089/services/server/status/resource-usage/splunk-processes</id>
 <updated>2014-03-26T13:35:52-07:00</updated>
```

```
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
   ... opensearch elements elided ...
<s:messages/>
<entry>
  <title>0</title>
  <id>https://localhost:8089/services/server/status/resource-usage/splunk-processes/0</id>
  <updated>2014-03-26T13:35:52-07:00</updated>
  <link href="/services/server/status/resource-usage/splunk-processes/0" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/status/resource-usage/splunk-processes/0" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="args"> instrument-resource-usage</s:key>
      <s:key name="eai:acl">
          ... elided ...
      </s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list/>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="elapsed">619262.3610</s:key>
      <s:key name="mem_used">15.762</s:key>
      <s:key name="page_faults">12001684</s:key>
      <s:key name="pct_memory">0.40</s:key>
      <s:key name="pid">4256</s:key>
      <s:key name="ppid">2476</s:key>
      <s:key name="process">splunkd</s:key>
      <s:key name="t_count">4</s:key>
    </s:dict>
  </content>
</entry>
```

server/sysinfo

`https://<host>:<mPort>/services/server/sysinfo`
Exposes relevant information about the resources and OS settings of the machine where Splunk Enterprise is running.

Usage details

This endpoint provides status information for the server where the current Splunk instance is running. The GET request response includes Kernel Transparent Huge Pages (THP) and `ulimit` status.

Note: Some properties returned by this endpoint are also returned by `server/info`. However, the `server/info` endpoint is meant to provide information on the currently running Splunk instance and not the machine where the instance is running. Server status values returned by `server/info` should be considered deprecated and might not continue to be accessible from this endpoint. Use the `server/sysinfo` endpoint for server information instead.

GET

Access server details.

Request parameters
None.

Returned values

Name	Description
cpu_arch	Server CPU architecture.
numberOfCores	Number of server processor cores. Not applicable if host is a VM guest. A value of `0` is returned if the number cannot be accessed and the access failure reason is logged to `splunkd.log`.
numberOfVirtualCores	Number of server virtual cores.
os_build	Software build for the server *os_version*.
os_name	Server operating system name.
os_name_extended	Server operating system name.
os_version	Server operating system version.
physicalMemoryMB	Server physical memory (MB). The same value is returned as the `mem` field from `server/status/resource-usage/hostwide`. A value of `0` is returned if the number cannot be accessed and the access failure reason is logged to `splunkd.log`.
transparent_hugepages	For Linux systems, includes the following THP status indicators. • `defrag` • `effective_state` • `enabled` For non-Linux systems, `effective_state` is set to `ok`
ulimits	On all UNIX systems, lists settings for the following `ulimits` in place on `splunkd` at runtime. • `core_file_size` • `cpu_time` • `data_file_size` • `data_segment_size` • `nice` • `open_files` • `resident_memory_size` • `stack_size` • `user_processes` • `virtual_address_space_size`

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/server/sysinfo
```

XML Response

```
...
  <title>system-info</title>
  <id>https://localhost:8089/services/server/sysinfo</id>
  <updated>2016-09-08T15:28:11-07:00</updated>
  <generator build="19e4b5854495" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/sysinfo/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>system-info</title>
    <id>https://localhost:8089/services/server/sysinfo/system-info</id>
    <updated>2016-09-08T15:28:11-07:00</updated>
    <link href="/services/server/sysinfo/system-info" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/sysinfo/system-info" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="cpu_arch">x86_64</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="numberOfCores">8</s:key>
        <s:key name="numberOfVirtualCores">8</s:key>
        <s:key name="os_build">#1 SMP Thu Feb 9 12:45:44 EST 2012</s:key>
        <s:key name="os_name">Linux</s:key>
        <s:key name="os_name_extended">Linux</s:key>
        <s:key name="os_version">2.6.18-274.18.1.el5</s:key>
        <s:key name="physicalMemoryMB">7982</s:key>
        <s:key name="transparent_hugepages">
          <s:dict>
            <s:key name="defrag"></s:key>
            <s:key name="effective_state">ok</s:key>
            <s:key name="enabled"></s:key>
          </s:dict>
        </s:key>
        <s:key name="ulimits">
          <s:dict>
            <s:key name="core_file_size">0</s:key>
            <s:key name="cpu_time">-1</s:key>
            <s:key name="data_file_size">-1</s:key>
            <s:key name="data_segment_size">-1</s:key>
            <s:key name="nice">0</s:key>
            <s:key name="open_files">1024</s:key>
            <s:key name="resident_memory_size">-1</s:key>
            <s:key name="stack_size">10485760</s:key>
            <s:key name="user_processes">73728</s:key>
            <s:key name="virtual_address_space_size">-1</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

services/saved/bookmarks/monitoring_console

`https://<host>:<mPort>/services/saved/bookmarks/monitoring_console`
Add URLs that link to monitoring consoles of your other deployments. For example, if you're admin overseeing multiple separate Splunk deployments for different teams.

GET

List deployment bookmarks.

Request parameters

Optional request parameters:

Name	Type	Description
count	Number	Number of bookmark URLs to list.
offset	Number	Lists bookmark URLs, offset from the first bookmark.
search	String	Items to search for, must be valid as SPL.
sort_dir	Enum	asc or desc; ascending or descending
sort_key	String	Key to sort on, must be existing key in the stanza

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/saved/bookmarks/monitoring_console
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bookmarks-mc</title>
  <id>https://qa-ubuntu-022:8089/services/saved/bookmarks/monitoring_console</id>
  <updated>2019-10-13T16:47:42-07:00</updated>
  <generator build="324da9f5a506" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
  <link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
  <link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment-2</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
```

```
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>deployment-3</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-3-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Add deployment bookmark URLs.

Request parameters

Name	Type	Description
name	String	Name of the deployment bookmark.
url	string	Full URL to the monitoring console of a different Splunk deployment.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/saved/bookmarks/monitoring_console -d
name=deployment-2 -d url=https://deployment-2-host:8000/en-US/app/splunk_monitoring_console
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bookmarks-mc</title>
  <id>https://localhost:8089/services/saved/bookmarks/monitoring_console</id>
  <updated>2019-10-13T16:16:38-07:00</updated>
  <generator build="324da9f5a506" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
  <link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
  <link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment-2</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2<
```

```
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

DELETE

Remove deployment bookmark URLs.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/saved/bookmarks/monitoring_console/{name}
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bookmarks-mc</title>
  <id>https://localhost:8089/services/saved/bookmarks/monitoring_console</id>
  <updated>2019-10-13T16:25:38-07:00</updated>
  <generator build="324da9f5a506" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
  <link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
  <link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment-2</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

Knowledge endpoints

Knowledge endpoint descriptions

Work with searches and other knowledge objects.

- Define data configurations indexed and searched by the Splunk platform.
- Manage how data is handled, using look-ups, field extractions, field aliases, sourcetypes, and transforms.
- Manage saved event types.
- Manage search field configurations and search time tags.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform URL for REST API access

Splunk Cloud Platform has a different host and management port syntax than Splunk Enterprise. Use the following URL for Splunk Cloud Platform deployments. If necessary, submit a support case using the Splunk Support Portal to open port 8089 on your deployment.

```
https://<deployment-name>.splunkcloud.com:8089
```

Free trial Splunk Cloud Platform accounts cannot access the REST API.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

admin/summarization

`https://<host>:<mPort>/services/admin/summarization/?by_tstats=1`
Get aggregated details about all accelerated data model summaries.

Authentication and authorization
Authorization to access data model acceleration information is role-based.

GET

Get a list of field:value pairs that provide details about accelerated data models and their summaries.

Request parameters
None.

Returned values

Name	Description
search	The data models, represented as search strings.
summary.access_count	The total number of times that the summary for each data model has been accessed.
summary.access_time	The last time that the summary of each data model was accessed.
summary.average_time	The average runtime of the past 48 summarization search jobs for this data model.
summary.buckets	The total number of buckets in the summaries of each data model.
summary.buckets_size	The total size of the buckets in the summaries of each data model. The size is reported in terms of megabytes (MB).
summary.complete	Reports whether or not the summaries for each data model are complete.
summary.earliest_time	The timestamp of the earliest event in the summaries for each data model.
summary.id	The ID of the data models being summarized. The format is `DM_<app_name>_<data_model_ID>`.
summary.is_inprogress	Indicates whether or not the summary build is currently in progress for each data model.
summary.last_error	Lists errors that were logged in the latest run (from `last_sid`) of the summary creation search.
summary.last_sid	The SID of the latest creation search job for each data model summary.
summary.latest_time	The timestamp of the latest events in each data model summary.
summary.latest_dispatch_time	The timestamp of the latest summary creation search for each data model.
summary.latest_run_duration	The runtime of the latest summary creation search for each data model.
summary.mod_time	The last time each data model summary was modified.
summary.p50	The 50th percentile of summarization search runtimes for each data model. 50 percent of the summarization searches for a given data model had runtimes that were less than this value.
summary.p90	The 90th percentile of summarization search runtimes for each data model. 90 percent of the summarization searches for a given data model had runtimes that were less than this value.
summary.run_stats	The start and duration of all saved previous summarization search jobs, up to 100 jobs.

Name	Description
summary.size	The total size of each summary, in bytes.
summary.time_range	The range of time covered by each summary.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/admin/summarization/?by_tstats=1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>summarization</title>
  <id>https://localhost:8089/services/admin/summarization</id>
  <updated>2015-06-01T15:21:20-07:00</updated>
  <generator build="e343948e242181aa7b94257ede83830605c853d9" version="20150526"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/summarization/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>tstats:DM_search_mydatamodel</title>
    <id>https://localhost:8089/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel<
/id>
    <updated>2015-06-01T15:21:20-07:00</updated>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel" rel="list"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel" rel="remove"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel/details"
rel="details"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel/reschedule"
rel="reschedule"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel/touch"
rel="touch"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms"/>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="search"><![CDATA[search search (index=* OR index=_*) (index=_internal) | eval nodename
= "rootevent"| eval is_Age=if(searchmatch("(avg_age)"),1,0), is_not_Age=1-is_Age | eval nodename =
if(nodename == "rootevent" AND searchmatch("(avg_age)"), mvappend(nodename, "rootevent.Age"), nodename) |
rename abandoned_channels AS rootevent.abandoned_channels average_kbps AS rootevent.average_kbps avg_age AS
rootevent.avg_age bytes AS rootevent.bytes clientip AS rootevent.clientip color AS rootevent.color
component AS rootevent.component cookie AS rootevent.cookie cpu_seconds AS rootevent.cpu_seconds
cumulative_hits AS rootevent.cumulative_hits current_queue_size AS rootevent.current_queue_size
current_size AS rootevent.current_size current_size_kb AS rootevent.current_size_kb date_hour AS
rootevent.date_hour is_Age AS rootevent.is_Age is_not_Age AS rootevent.is_not_Age | fields nodename, _time,
host, source, sourcetype, rootevent.abandoned_channels, rootevent.average_kbps, rootevent.avg_age,
rootevent.bytes, rootevent.clientip, rootevent.color, rootevent.component, rootevent.cookie,
rootevent.cpu_seconds, rootevent.cumulative_hits, rootevent.current_queue_size, rootevent.current_size,
rootevent.current_size_kb, rootevent.date_hour, rootevent.is_Age, rootevent.is_not_Age]]></s:key>
        <s:key name="summary.access_count">0</s:key>
        <s:key name="summary.access_time">0</s:key>
        <s:key name="summary.buckets">22</s:key>
        <s:key name="summary.buckets_size">273</s:key>
        <s:key name="summary.complete">1.000000</s:key>
        <s:key name="summary.earliest_time">1432174156</s:key>
        <s:key name="summary.id">DM_search_mydatamodel</s:key>
        <s:key name="summary.is_inprogress">0</s:key>
        <s:key name="summary.last_error"></s:key>
        <s:key
name="summary.last_sid">scheduler__nobody__search__RMD5692d85674596d683_at_1433197200_18815</s:key>
        <s:key name="summary.latest_time">1432684089</s:key>
        <s:key name="summary.mod_time">1433196908</s:key>
        <s:key name="summary.size">61153280</s:key>
        <s:key name="summary.time_range">604800</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

admin/summarization/tstats:DM_{app}_{data_model_ID}

`https://<host>:<mPort>/services/admin/summarization/tstats:DM_{app}_{data_model_ID}`

Review information about the summaries of a specific data model. Identify specific data models by providing their app short name and their data model ID.

Authentication and authorization

Authorization to access data model acceleration information is role-based.

GET

Get detailed information about the acceleration summaries of a specific datamodel. See statistics about data model usage and information about the latest summary creation run.

Request parameters

Name	Type	Default	Description

app required	string		The short name of the app to which the data set belongs.
data model ID required	string		The ID of the data model.

Returned values

Name	Description
search	The data model, represented as a search string.
summary.access_count	The total number of times that the summary for this data model has been accessed.
summary.access_time	The last time that the summary of this data model was accessed.
summary.average_time	The average runtime of the past 48 summarization search jobs for this data model.
summary.buckets	The total number of buckets in the summary of this data model.
summary.buckets_size	The total size of the buckets in the summary of this data model. The size is reported in terms of megabytes (MB).
summary.complete	Reports whether or not the summary for the data model are complete.
summary.earliest_time	The timestamp of the earliest event in the summary for this data model.
summary.id	The ID of the data model being summarized. The format is `DM_<app_name>_<data_model_ID>`.
summary.is_inprogress	Indicates whether or not the data model summary build is currently in progress.
summary.last_error	Lists errors that were logged in the latest run (from `last_sid`) of the summary creation search.
summary.last_sid	The SID of the latest data model summary creation search job.
summary.latest_time	The timestamp of the latest event in the data model summary.
summary.latest_dispatch_time	The timestamp of the latest summary creation search for the data model.
summary.latest_run_duration	The runtime of the latest summary creation search for the data model.
summary.mod_time	The last time the data model summary was modified.
summary.p50	The 50th percentile of summarization search runtimes for the data model. 50 percent of the summarization searches for this data model had runtimes that were less than this value.
summary.p90	The 90th percentile of summarization search runtimes for the data model. 90 percent of the summarization searches for this data model had runtimes that were less than this value.
summary.run_stats	The start and duration of all saved previous summarization search jobs, up to 100 jobs.
summary.size	The total size of the summary, in bytes.
summary.time_range	The range of time covered by the summary.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/admin/summarization/tstats:DM_search_test_new_accel
```

XML Response

```
...
<title>summarization</title>
<id>https://localhost:1413/servicesNS/nobody/search/admin/summarization</id>
<updated>2019-08-13T14:58:12-07:00</updated>
<generator build="2ec8251a07e11294725aa6800463f8a975e18641" version="20190809"/>
<author>
<name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>tstats:DM_search_test_new_accel</title>
<id>https://localhost:1413/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel"
rel="alternate"/>
<author>
<name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel" rel="list"/>
<link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel" rel="remove"/>
<link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel/details"
rel="details"/>
<link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel/reschedule"
rel="reschedule"/>
<link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_test_new_accel/touch"
rel="touch"/>
<content type="text/xml">
<s:dict>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms"/>
<s:key name="removable">0</s:key>
<s:key name="sharing">user</s:key>
</s:dict>
</s:key>
<s:key name="eai:attributes">
<s:dict>
<s:key name="optionalFields">
<s:list>
<s:item>isProxyRequest</s:item>
<s:item>noProxy</s:item>
<s:item>time_format</s:item>
</s:list>
</s:key>
<s:key name="requiredFields">
<s:list/>
</s:key>
<s:key name="wildcardFields">
<s:list/>
</s:key>
</s:dict>
</s:key>
<s:key name="search">search search (index=* OR index=_*) (index=_internal date_second=31) | eval nodename =
"test" | fields nodename, _time, host, source, sourcetype</s:key>
<s:key name="summary.access_count">0</s:key>
<s:key name="summary.access_time">0</s:key>
<s:key name="summary.average_time">3.028</s:key>
<s:key name="summary.buckets">11</s:key>
<s:key name="summary.buckets_size">461</s:key>
<s:key name="summary.complete">1</s:key>
<s:key name="summary.earliest_time">1565398764</s:key>
<s:key name="summary.id">DM_search_test_new_accel</s:key>
<s:key name="summary.is_inprogress">0</s:key>
<s:key name="summary.last_error">[ronnie.sv.splunk.com] A second test error message just because.
[ronnie.sv.splunk.com] Test error message in remote server.</s:key>
<s:key name="summary.last_sid">scheduler__nobody__search__RMD5837da1d4b8a764d1_at_1565733480_379</s:key>
<s:key name="summary.latest_dispatch_time">1565733481</s:key>
<s:key name="summary.latest_run_duration">5.691</s:key>
<s:key name="summary.latest_time">1565730106</s:key>
<s:key name="summary.mod_time">1565733421</s:key>
<s:key name="summary.p50">1.287</s:key>
<s:key name="summary.p90">5.859</s:key>
<s:key name="summary.run_stats">
<s:dict>
<s:key name="1565730661">
<s:dict>
<s:key name="dispatch_time">1565730661</s:key>
<s:key name="run_duration">0.357</s:key>
</s:dict>
</s:key>
<s:key name="1565730721">
<s:dict>
<s:key name="dispatch_time">1565730721</s:key>
<s:key name="run_duration">0.240</s:key>
</s:dict>
</s:key>
<s:key name="1565730780">
<s:dict>
<s:key name="dispatch_time">1565730780</s:key>
<s:key name="run_duration">0.253</s:key>
</s:dict>
</s:key>
<s:key name="1565730840">
<s:dict>
<s:key name="dispatch_time">1565730840</s:key>
<s:key name="run_duration">0.247</s:key>
</s:dict>
</s:key>
<s:key name="1565730900">
<s:dict>
<s:key name="dispatch_time">1565730900</s:key>
<s:key name="run_duration">0.233</s:key>
</s:dict>
</s:key>
<s:key name="1565730960">
<s:dict>
<s:key name="dispatch_time">1565730960</s:key>
<s:key name="run_duration">0.266</s:key>
</s:dict>
</s:key>
<s:key name="1565731020">
<s:dict>
<s:key name="dispatch_time">1565731020</s:key>
<s:key name="run_duration">0.268</s:key>
</s:dict>
```

```
</s:key>
</s:dict>
</s:key>
<s:key name="summary.size">614400</s:key>
<s:key name="summary.time_range">86400</s:key>
</s:dict>
</content>
</entry>
</feed>
```

data/lookup-table-files

```
https://<host>:<mPort>/services/data/lookup-table-files/
```

Access lookup table files.

This endpoint is available only in Splunk Enterprise.

GET

List lookup table files.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
eai:appName	The app for which the lookup table applies.
eai:data	The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.
eai:userName	The Splunk user who created the lookup table.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/lookup-table-files
```

XML Response

```
...
 <title>lookup-table-files</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
  <updated>2011-07-21T19:26:11-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>lookup.csv</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>
    <updated>2011-07-21T19:26:11-07:00</updated>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="list"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="edit"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="remove"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl nodes elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:data">
<![CDATA[/opt/splunk/etc/users/admin/search/lookups/lookup.csv]]>        </s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a lookup table file by moving a file from the upload staging area into $SPLUNK_HOME.

Request parameters

Name	Type	Default	Description
eai:data required	String		Move a lookup table file from the given path into $SPLUNK_HOME. This path must have the lookup staging area as an ancestor.
name required	String		The lookup table filename.

Returned values

Name	Description
eai:appName	The app for which the lookup table applies.
eai:data	The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.
eai:userName	The Splunk user who created the lookup table.

Name	Description

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/lookup-table-files -d
eai:data=/opt/splunk/var/run/splunk/lookup_tmp/lookup-in-staging-dir.csv -d name=lookup.csv
```

XML Response

```
...
<title>lookup-table-files</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
  <updated>2011-07-21T18:26:35-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>lookup.csv</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>
    <updated>2011-07-21T18:26:35-07:00</updated>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="list"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="edit"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="remove"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:data">
<![CDATA[/opt/splunk/etc/users/admin/search/lookups/lookup.csv]]>        </s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/lookup-table-files/{name}

https://<host>:<mPort>/services/data/lookup-table-files/{name}

Manage the `{name}` lookup table file.

This endpoint is available only in Splunk Enterprise.

DELETE

Delete the named lookup table file.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>lookup-table-files</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
  <updated>2011-07-21T18:43:11-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

List a single lookup table file.

Request parameters

None

Returned values

Name	Description
eai:appName	The app for which the lookup table applies.
eai:attributes	Field control information.
eai:data	The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.
eai:userName	The Splunk user who created the lookup table.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv
```

XML Response

```
...
 <title>lookup-table-files</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
  <updated>2011-07-21T18:37:25-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>lookup.csv</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>
    <updated>2011-07-21T18:37:25-07:00</updated>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="list"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="edit"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="remove"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>eai:data</s:item>
            </s:list>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:data">
<![CDATA[/opt/splunk/etc/users/admin/search/lookups/lookup.csv]]>        </s:key>
      <s:key name="eai:userName">admin</s:key>
    </s:dict>
  </content>
 </entry>
</feed>
```

POST

Modify a lookup table file by replacing it with a file from the upload staging area.

Request parameters

Name	Type	Default	Description
eai:data required	String		Move a lookup table file from the given path into $SPLUNK_HOME. This path must have the lookup staging area as an ancestor.

Returned values

Name	Description
eai:appName	The app for which the lookup table applies.
eai:data	The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.
eai:userName	The Splunk user who created the lookup table.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv -d
eai:data=/opt/splunk/var/run/splunk/lookup_tmp/another-lookup-in-staging-dir.csv
```

XML Response

```
...
  <title>lookup-table-files</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
  <updated>2011-07-21T18:41:52-07:00</updated>
  <generator version="104309"/>
  <author>
```

```
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>lookup.csv</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>
    <updated>2011-07-21T18:41:52-07:00</updated>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="list"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="edit"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="remove"/>
    <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:data">
<![CDATA[/opt/splunk/etc/users/admin/search/lookups/lookup.csv]]>        </s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/calcfields

```
https://<host>:<mPort>/services/data/props/calcfields
```

Provides access to calculated fields, which are eval expressions in props.conf.

GET

Returns information on calculated fields for this instance of your Splunk deployment.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
attribute	The name of the calculated field, which includes the "EVAL-" prefix.

Name	Description
field.name	The name of the field which is being calculated with an EVAL expression.
stanza	The name of the stanza in props.conf that defines the calculated field.
type	The type of the calculated field. This is always EVAL.
value	The EVAL statement for the calculated field.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/data/props/calcfields
```

XML Response

```
 <title>props-eval</title>
  <id>https://localhost:8089/services/data/props/calcfields</id>
  <updated>2012-10-01T15:01:50-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/props/calcfields/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title><access_common> : EVAL-response_time</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL
-response_time</id>
    <updated>2012-10-01T15:01:50-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EVAL-response_time</s:key>
        ... eai:acl node elided ...
        <s:key name="field.name">response_time</s:key>
        <s:key name="stanza"><access_common></s:key>
        <s:key name="type">EVAL</s:key>
        <s:key name="value">response_time/1000</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create an eval expression defining a calculated field in props.conf.

See Create a calculated field by editing props.conf in the *Knowledge Manager Manual* for more details.

Request parameters

Name	Type	Default	Description
name required	String		The name of the calculated field. Do not specify the "EVAL-" prefix for the field. When Splunk software writes the calculated field to props.conf, it adds the "EVAL-" prefix.
stanza required	String		The name of the stanza in props.conf for the calculated field. The name can be any of the following: • Sourcetype of an event • host::<host>, where <host> is the host for an event • source::<source>, where <source> is the source for an event. **Note:** Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.
value required	String		The eval statement, which can be evaluated to any value type, including multivals, boolean, or null. **Note:** Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.

Returned values

Name	Description
attribute	The name of the calculated field, which includes the "EVAL-" prefix.
field.name	The name of the field which is being calculated with an EVAL expression.
stanza	The name of the stanza in props.conf that defines the calculated field.
type	The type of the calculated field. This is always EVAL.

Name	Description
value	The EVAL statement for the calculated field.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/data/props/calcfields -d name=response_time -d
stanza=%3Caccess_common%3E -d value=response_time/1000
```

XML Response

```
...
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>props-eval</title>
  <id>https://localhost:8089/services/data/props/calcfields</id>
  <updated>2012-10-01T14:58:45-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/props/calcfields/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title><access_common> : EVAL-response_time</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL
-response_time</id>
    <updated>2012-10-01T14:58:45-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EVAL-response_time</s:key>
        ... eai:acl node elided ...
        <s:key name="field.name">response_time</s:key>
        <s:key name="stanza"><access_common></s:key>
        <s:key name="type">EVAL</s:key>
        <s:key name="value">response_time/1000</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/calcfields/{name}

`https://<host>:<mPort>/services/data/props/calcfields/{name}`

Manage the `{name}` calculated field.

DELETE

Deletes the named calculated field.

Usage details

Use URL-encoding to ensure that Splunk software interprets the name of the calculated field correctly.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>props-eval</title>
  <id>https://localhost:8089/services/data/props/calcfields</id>
  <updated>2012-10-01T15:33:06-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/props/calcfields/_new" rel="create"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

GET

Access the named calculated field.

Request parameters

None

Returned values

Name	Description
attribute	The name of the calculated field, which includes the "EVAL-" prefix.
field.name	The name of the field which is being calculated with an EVAL expression.
stanza	The name of the stanza in props.conf that defines the calculated field.
type	The type of the calculated field. This is always EVAL.
value	The EVAL statement for the calculated field.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time
```

XML Response

```
<title>props-eval</title>
  <id>https://localhost:8089/services/data/props/calcfields</id>
  <updated>2012-10-01T15:05:09-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/props/calcfields/_new" rel="create"/>
  ... opensearch nodes elided ...
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
```

```
    <title><access_common> : EVAL-response_time</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL
-response_time</id>
    <updated>2012-10-01T15:05:09-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EVAL-response_time</s:key>
        ... eai:acl node elided ...
        ... eai:attributes node elided ...
        <s:key name="field.name">response_time</s:key>
        <s:key name="stanza"><access_common></s:key>
        <s:key name="type">EVAL</s:key>
        <s:key name="value">response_time/1000</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update the named calculated field.

Request parameters

Name	Type	Default	Description
value	String		The eval statement, which can be evaluated to any value type, including multivals, boolean, or null. *Note:* Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly. See Create a calculated field by editing props.conf in the *Knowledge Manager Manual* for details.

Returned values

Name	Description
attribute	The name of the calculated field, which includes the "EVAL-" prefix.
field.name	The name of the field which is being calculated with an EVAL expression.
stanza	The name of the stanza in props.conf that defines the calculated field.
type	The type of the calculated field. This is always EVAL.
value	The EVAL statement for the calculated field.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time -d
value=response_time/100
```

XML Response

```
<title>props-eval</title>
  <id>https://localhost:8089/services/data/props/calcfields</id>
  <updated>2012-10-01T15:14:19-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/props/calcfields/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title><access_common> : EVAL-response_time</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL
-response_time</id>
    <updated>2012-10-01T15:14:19-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move"
rel="move"/>
```

```
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EVAL-response_time</s:key>
        ... eai:acl node elided ...
        <s:key name="field.name">response_time</s:key>
        <s:key name="stanza"><access_common></s:key>
        <s:key name="type">EVAL</s:key>
        <s:key name="value">response_time/100</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/extractions

```
https://<host>:<mPort>/services/data/props/extractions
```

GET

List field extractions.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	The props.conf stanza to which this field extraction applies. for example, the sourcetype or source that triggers this field extraction. The full name of the field extraction includes this stanza name as a prefix.
type	Specifies the field extraction type, which can be either `inline` or `uses transform`.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/extractions
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T22:55:04-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>access_combined : REPORT-access</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/props/extractions/access_combined%20%3A%20REPORT
-access</id>
    <updated>2011-07-10T22:55:04-07:00</updated>
    <link href="/servicesNS/nobody/system/data/props/extractions/access_combined%20%3A%20REPORT-access"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/props/extractions/access_combined%20%3A%20REPORT-access"
rel="list"/>
    <link href="/servicesNS/nobody/system/data/props/extractions/access_combined%20%3A%20REPORT-access"
rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">REPORT-access</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">access_combined</s:key>
        <s:key name="type">Uses transform</s:key>
        <s:key name="value">access-extractions</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new field extraction.

Request parameters

Name	Type	Default	Description
name required	String		The user-specified part of the field extraction name. The full name of the field extraction includes this identifier as a suffix.
stanza required	String		The props.conf stanza to which this field extraction applies, e.g. the sourcetype or source that triggers this field extraction. The full name of the field extraction includes this stanza name as a prefix.
type required	Enum		Valid values: (REPORT | EXTRACT)

Name	Type	Default	Description
			An EXTRACT-type field extraction is defined with an "inline" regular expression. A REPORT-type field extraction refers to a transforms.conf stanza.
value required	String		If this is an EXTRACT-type field extraction, specify a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, specify a comma- or space-delimited list of transforms.conf stanza names that define the field transformations to apply.

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	Specifies the name of the stanza for the field extraction.
type	Specifies the field extraction type, which can be either `inline` or `uses transform`.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/extractions -d name=port -d
stanza=ftp_log -d type=EXTRACT -d "value=port (?<port_number>\d+)"
```

XML Response

```
...
 <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T22:56:17-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>ftp_log : EXTRACT-port</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port<
/id>
    <updated>2011-07-10T22:56:17-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EXTRACT-port</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">ftp_log</s:key>
        <s:key name="type">Inline</s:key>
        <s:key name="value">port (?<port_number>\d )</s:key>
      </s:dict>
    </content>
  </entry>
```

data/props/extractions/{name}

```
https://<host>:<mPort>/services/data/props/extractions/{name}
```

Manage the `{name}` field extraction.

DELETE

Delete the named field extraction.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T23:05:42-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

List a single field extraction.

Request parameters

None

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	The props.conf stanza to which this field extraction applies. for example, the sourcetype or source that triggers this field extraction. The full name of the field extraction includes this stanza name as a prefix.
type	Specifies the field extraction type, which can be either `inline` or `uses transform`.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T23:02:31-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>ftp_log : EXTRACT-port</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port<
/id>
    <updated>2011-07-10T23:02:31-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EXTRACT-port</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>value</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="stanza">ftp_log</s:key>
        <s:key name="type">Inline</s:key>
        <s:key name="value">connection on port (?<port_number>\d )</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Modify the named field extraction.

Request parameters

Name	Type	Default	Description
value required	String		If this is an EXTRACT-type field extraction, specify a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, specify a comma- or space-delimited list of transforms.conf stanza names that define the field transformations to apply.

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	Specifies the name of the stanza for the field extraction.
type	Specifies the field extraction type, which can be either `inline` or `uses transform`.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port -d
"value=connection on port (?<port_number>\d+)"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T23:05:05-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>ftp_log : EXTRACT-port</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port<
/id>
    <updated>2011-07-10T23:05:05-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">EXTRACT-port</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">ftp_log</s:key>
        <s:key name="type">Inline</s:key>
        <s:key name="value">connection on port (?<port_number>\d )</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/fieldaliases

`https://<host>:<mPort>/services/data/props/fieldaliases`
Access or create field aliases.

GET

List field aliases.

Example

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
*alias.**	The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.
type	Specifies the field extraction type, which can be either `inline` or `uses transform`.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:31:41-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : FIELDALIAS-alias_name</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my
_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
    <updated>2011-07-21T19:31:41-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="alias.foo">bar</s:key>
        <s:key name="attribute">FIELDALIAS-alias_name</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="type">FIELDALIAS</s:key>
        <s:key name="value">foo AS bar</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new field alias.

Name	Type	Default	Description
*alias.**	String		The alias for a given field. For example, supply a value of "bar" for an argument "alias.foo" to alias "foo" to "bar".
name required	String		The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
stanza required	String		The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.

Returned values

Name	Description
*alias.**	The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.
type	Specifies the field extraction type, which can be either inline or uses transform.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases -d
name=alias_name -d stanza=my_sourcetype -d alias.foo=bar
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:30:17-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : FIELDALIAS-alias_name</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my
_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
    <updated>2011-07-21T19:30:17-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="alias.foo">bar</s:key>
        <s:key name="attribute">FIELDALIAS-alias_name</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="type">FIELDALIAS</s:key>
        <s:key name="value">foo AS bar</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/fieldaliases/{name}

`https://<host>:<mPort>/services/data/props/fieldaliases/{name}`

Manage the `{name}` field alias.

DELETE

Delete the named field alias.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:37:45-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access a field alias.

Request parameters

None

Returned values

Name	Description
*alias.**	The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.
type	Specifies the field extraction type, which can be either `inline` or `uses transform`.

Name	Description
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:33:00-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : FIELDALIAS-alias_name</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my
_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
    <updated>2011-07-21T19:33:00-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="alias.foo">bar</s:key>
        <s:key name="attribute">FIELDALIAS-alias_name</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>alias\..*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="type">FIELDALIAS</s:key>
        <s:key name="value">foo AS bar</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update a field alias.

Request parameters

Name	Type	Default	Description
*alias.**	String		The alias for a given field. For example, supply a value of "bar" for an argument "alias.foo" to alias "foo" to "bar".

Returned values

Name	Description
*alias.**	The alias for a given field. For example, supply a value of "bar" for an argument "alias.foo" to alias "foo" to "bar".
attribute	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
stanza	The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.
type	Specifies the field extraction type, which can be either inline or uses transform.
value	If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name
-d alias.hi=hello -d alias.bye=goodbye
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:34:36-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : FIELDALIAS-alias_name</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my
_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
    <updated>2011-07-21T19:34:36-07:00</updated>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="list"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="edit"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name"
rel="remove"/>
    <link
href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="alias.bye">goodbye</s:key>
        <s:key name="alias.hi">hello</s:key>
        <s:key name="attribute">FIELDALIAS-alias_name</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="type">FIELDALIAS</s:key>
        <s:key name="value">bye AS goodbye hi AS hello</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/lookups

`https://<host>:<mPort>/services/data/props/lookups`
Access or create automatic lookups.

GET

List automatic lookups.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, LOOKUP-my_lookup.
overwrite	If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.
stanza	The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.
transform	The transforms.conf stanza that defines the lookup to apply.
type	Specifies the field extraction type. For this endpoint, this is always `LOOKUP`
value	The transform stanza with the value for the lookup.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/lookups
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:43:53-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : LOOKUP-my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my
_lookup</id>
    <updated>2011-08-01T20:43:53-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="list"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">LOOKUP-my_lookup</s:key>
        ... eai:acl node elided ...
        <s:key name="lookup.field.input.foo"/>
        <s:key name="lookup.field.output.fuzz"/>
        <s:key name="overwrite">1</s:key>
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="transform">my_transform</s:key>
        <s:key name="type">LOOKUP</s:key>
        <s:key name="value">my_transform foo OUTPUT fuzz</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create an automatic lookup.

Request parameters

Name	Type	Default	Description
*lookup.field.input.**	String		A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.
*lookup.field.output.**	String		A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.

Name	Type	Default	Description
name required	String		The user-specified part of the automatic lookup name. The full name of the automatic lookup includes this identifier as a suffix.
overwrite required	Boolean		If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.
stanza required	String		The props.conf stanza to which this automatic lookup applies, e.g. the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.
transform required	String		The transforms.conf stanza that defines the lookup to apply.

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, LOOKUP-my_lookup.
*lookup.field.input.**	A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.
*lookup.field.output.**	A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.
overwrite	If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.
stanza	The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.
transform	The transforms.conf stanza that defines the lookup to apply.
type	Specifies the field extraction type. For this endpoint, this is alwqys `LOOKUP`.
value	The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/lookups -d name=my_lookup -d
overwrite=1 -d stanza=my_sourcetype -d transform=my_transform -d lookup.field.input.foo= -d
lookup.field.output.fuzz=
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:43:31-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : LOOKUP-my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my
_lookup</id>
    <updated>2011-08-01T20:43:31-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="list"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">LOOKUP-my_lookup</s:key>
        ... eai:acl node elided ...
        <s:key name="lookup.field.input.foo"/>
        <s:key name="lookup.field.output.fuzz"/>
        <s:key name="overwrite">1</s:key>
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="transform">my_transform</s:key>
        <s:key name="type">LOOKUP</s:key>
        <s:key name="value">my_transform foo OUTPUT fuzz</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/lookups/{name}

`https://<host>:<mPort>/services/data/props/lookups/{name}`

Manage the `{name}` automatic lookup.

DELETE

Delete an automatic lookup.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:44:32-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access an automatic lookup.

Request parameters

None

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, LOOKUP-my_lookup.
overwrite	If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.
stanza	The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.
transform	The transforms.conf stanza that defines the lookup to apply.
type	Specifies the field extraction type. For this endpoint, this is always `LOOKUP`.
value	The transform stanza with the value for the lookup.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:44:06-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : LOOKUP-my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my
_lookup</id>
    <updated>2011-08-01T20:44:06-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="list"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="edit"/>
```

```
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">LOOKUP-my_lookup</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>overwrite</s:item>
                <s:item>transform</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>lookup\.field\.input\..*</s:item>
                <s:item>lookup\.field\.output\..*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="lookup.field.input.foo"/>
        <s:key name="lookup.field.output.fuzz"/>
        <s:key name="overwrite">1</s:key>
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="transform">my_transform</s:key>
        <s:key name="type">LOOKUP</s:key>
        <s:key name="value">my_transform foo OUTPUT fuzz</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update an automatic lookup.

Request parameters

Name	Type	Default	Description
*lookup.field.input.**	String		A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.
*lookup.field.output.**	String		A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.
overwrite required	Boolean		If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.

Name	Type	Default	Description
transform required	String		The transforms.conf stanza that defines the lookup to apply.

Returned values

Name	Description
attribute	Specifies the field extraction configuration. For example, LOOKUP-my_lookup.
*lookup.field.input.**	A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.
*lookup.field.output.**	A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.
overwrite	If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.
stanza	The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.
transform	The transforms.conf stanza that defines the lookup to apply.
type	Specifies the field extraction type. For this endpoint, this is alwqys `LOOKUP`.
value	The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup -d
overwrite=1 -d transform=other_transform -d lookup.field.input.bar= -d lookup.field.output.buzz=
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:44:21-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : LOOKUP-my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my
_lookup</id>
    <updated>2011-08-01T20:44:21-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="list"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup"
rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup/move"
rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">LOOKUP-my_lookup</s:key>
        ... eai:acl node elided ...
        <s:key name="lookup.field.input.bar"/>
        <s:key name="lookup.field.output.buzz"/>
        <s:key name="overwrite">1</s:key>
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="transform">other_transform</s:key>
        <s:key name="type">LOOKUP</s:key>
        <s:key name="value">other_transform bar OUTPUT buzz</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/sourcetype-rename

`https://<host>:<mPort>/services/data/props/sourcetype-rename`

Access or rename `props.conf` sourcetypes.

GET

List renamed sourcetypes.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
attribute	The configuration key.
stanza	The sourcetype to rename, which is the name of a stanza in props.conf.
type	The value of the configuration key.
value	The new name for the sourcetype.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:40:53-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>hardware</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
    <updated>2011-07-12T15:40:53-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">rename</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">hardware</s:key>
        <s:key name="type">rename</s:key>
        <s:key name="value">hw</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Rename a sourcetype.

Request parameters

Name	Type	Default	Description
name required	String		The original sourcetype name.
value required	String		The new sourcetype name.

Returned values

Name	Description
attribute	The configuration key.
stanza	The sourcetype to rename, which is the name of a stanza in props.conf.
type	The value of the configuration key.
value	The new name for the sourcetype.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename -d
name=hardware -d value=hw
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:39:57-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>hardware</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
    <updated>2011-07-12T15:39:57-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
    <author>
```

```
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">rename</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">hardware</s:key>
        <s:key name="type">rename</s:key>
        <s:key name="value">hw</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/props/sourcetype-rename/{name}

`https://<host>:<mPort>/services/data/props/sourcetype-rename/{name}`
Access, delete, or update a sourcetype name.

DELETE

Restore the original sourcetype name for `{name}`.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:49:16-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access a specific renamed sourcetype.

Request parameters

None

Returned values

Name	Description
attribute	The configuration key.
stanza	The sourcetype to rename, which is the name of a stanza in props.conf.
type	The value of the configuration key.
value	The new name for the sourcetype.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:44:47-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>hardware</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
    <updated>2011-07-12T15:44:47-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">rename</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>value</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="stanza">hardware</s:key>
        <s:key name="type">rename</s:key>
        <s:key name="value">hw</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update a renamed sourcetype name.

Request parameters

Name	Type	Default	Description
value required	String		The new sourcetype name.

Returned values

Name	Description
attribute	The configuration key.
stanza	The sourcetype to rename, which is the name of a stanza in props.conf.
type	The value of the configuration key.
value	The new name for the sourcetype.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware
-d value=hrdwr
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:46:58-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>hardware</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
    <updated>2011-07-12T15:46:58-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">rename</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">hardware</s:key>
        <s:key name="type">rename</s:key>
        <s:key name="value">hrdwr</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/transforms/extractions

`https://<host>:<mPort>/services/data/transforms/extractions`

Access field extraction definitions.

GET

List field extractions.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms.

Name	Description
	For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
disabled	Indicates if the field transformation is disabled.
eai:appName	The Splunk app for which the field extractions are defined. For example, the search app.
eai:userName	The name of the Splunk user who created the field extraction definitions. For example, the admin user.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/extractions
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:28:03-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>access-extractions</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/transforms/extractions/access-extractions</id>
    <updated>2011-07-21T20:28:03-07:00</updated>
    <link href="/servicesNS/nobody/system/data/transforms/extractions/access-extractions" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/nobody/system/data/transforms/extractions/access-extractions" rel="list"/>
    <link href="/servicesNS/nobody/system/data/transforms/extractions/access-extractions/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/transforms/extractions/access-extractions" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/transforms/extractions/access-extractions/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">1</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX">
<![CDATA[^[[nspaces:clientip]]\s++[[nspaces:ident]]\s++[[nspaces:user]]\s++[[sbstring:req_time]]\s++[[access
-request]]\s++[[nspaces:status]]\s++[[nspaces:bytes]](?:\s++"(?<referer>[[bc_domain:referer
_]]?+[^"]*+)"(?:\s++[[qstring:useragent]](?:\s++[[qstring:cookie]])?+)?+)?[[all:other]]]]>        </s:key>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a new field transformation.

Request parameters

Name	Type	Default	Description
CAN_OPTIMIZE	Bool	True	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is needed for the successful evaluation of a search. NOTE: This option should rarely be set to false.
CLEAN_KEYS	Boolean	True	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
disabled	Boolean		Specifies whether the field transformation is disabled.
FORMAT	String		This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. FORMAT for index-time extractions: Use $n (for example $1, $2, etc) to specify the output of each REGEX match. If REGEX does not have n groups, the matching fails.

Name	Type	Default	Description
			The special identifier $0 represents what was in the DEST_KEY before the REGEX was performed. At index-time only, you can use FORMAT to create concatenated fields: FORMAT = ipaddress::$1.$2.$3.$4 When you create concatenated fields with FORMAT, "$" is the only special character. It is treated as a prefix for regex-capturing groups only if it is followed by a number and only if the number applies to an existing capturing group. So if REGEX has only one capturing group and its value is "bar", then: \t"FORMAT = foo$1" yields "foobar" \t"FORMAT = foo$bar" yields "foo$bar" \t"FORMAT = foo$1234" yields "foo$1234" \t"FORMAT = foo$1\\$2" yields "foobar\\$2" At index-time, FORMAT defaults to <stanza-name>::$1 FORMAT for search-time extractions: The format of this field as used during search time extractions is as follows: \tFORMAT = <field-name>::<field-value>(<field-name>::<field-value>)* \tfield-name = [<string>\|$<extracting-group-number>] \tfield-value = [<string>|$<extracting-group-number>] Search-time extraction examples: \tFORMAT = first::$1 second::$2 third::other-value \tFORMAT = $1::$2 You cannot create concatenated fields with FORMAT at search time. That functionality is only available at index time. At search-time, FORMAT defaults to an empty string.
KEEP_EMPTY_VALS	Boolean	False	If set to true, Splunk software preserves extracted fields with empty values.
MV_ADD	Boolean	False	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
name required	String		The name of the field transformation.
REGEX required	String		Specify a regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: \tREGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). \tREGEX is required for all index-time transforms. REGEX and the FORMAT attribute: Name-capturing groups in the REGEX are extracted directly to fields. This means that you do not need to specify the FORMAT attribute for simple field extraction cases.

Name	Type	Default	Description
			If the REGEX extracts both the field name and its corresponding field value, you can use the following special capturing groups if you want to skip specifying the mapping in FORMAT: _KEY_<string>, _VAL_<string>. For example, the following are equivalent: \tUsing FORMAT: \t\tREGEX = ([a-z]+)=([a-z]+) \t\tFORMAT = $1::$2 \tWithout using FORMAT \t\tREGEX = (?<_KEY_1>[a-z]+)=(?<_VAL_1>[a-z]+) REGEX defaults to an empty string.
SOURCE_KEY required	String	_raw	Specify the KEY to which Splunk software applies REGEX.

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: \\tREGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). \\tREGEX is required for all index-time transforms.

Name	Description
	For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
disabled	Indicates if the field transformation is disabled.
eai:appName	The Splunk app for which the field extractions are defined. For example, the search app.
eai:userName	The name of the Splunk user who created the field extraction definitions. For example, the admin user.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/extractions -d
REGEX="(?<_KEY_1>[a-z]*),(?<_VAL_1>[a-z]*)" -d SOURCE_KEY=_raw -d name=my_transform
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:25:20-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_transform</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform</id>
    <updated>2011-07-21T20:25:20-07:00</updated>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">1</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX">(?<_KEY_1>[a-z]*),(?<_VAL_1>[a-z]*)</s:key>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/transforms/extractions/{name}

`https://<host>:<mPort>/services/data/transforms/extractions/{name}`

Access, delete, or update the `{name}` field extraction.

DELETE

Delete a field extraction.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:34:30-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access a specific field extraction.

Request parameters

None

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event.

Name	Description
	Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
disabled	Indicates if the field transformation is disabled.
eai:appName	The Splunk app for which the field extractions are defined. For example, the search app.
eai:attributes	Field control information.
eai:userName	The name of the Splunk user who created the field extraction definitions. For example, the admin user.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:29:00-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_transform</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform</id>
    <updated>2011-07-21T20:29:00-07:00</updated>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">1</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX">(?<_KEY_1>[a-z]*),(?<_VAL_1>[a-z]*)</s:key>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>CAN_OPTIMIZE</s:item>
                <s:item>CLEAN_KEYS</s:item>
                <s:item>FORMAT</s:item>
                <s:item>KEEP_EMPTY_VALS</s:item>
                <s:item>MV_ADD</s:item>
                <s:item>disabled</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>REGEX</s:item>
                <s:item>SOURCE_KEY</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update a field extraction.

Request parameters

Name	Type	Default	Description
REGEX	String		Specify a regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: \tREGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). \tREGEX is required for all index-time transforms. REGEX and the FORMAT attribute: Name-capturing groups in the REGEX are extracted directly to fields. This means that you do not need to specify the FORMAT attribute for simple field extraction cases. If the REGEX extracts both the field name and its corresponding field value, you can use the following special capturing groups if you want to skip specifying the mapping in FORMAT: _KEY_<string>, _VAL_<string>. For example, the following are equivalent: \tUsing FORMAT: \t\tREGEX = ([a-z]+)=([a-z]+) \t\tFORMAT = $1::$2 \tWithout using FORMAT \t\tREGEX = (?<_KEY_1>[a-z]+)=(?<_VAL_1>[a-z]+) REGEX defaults to an empty string.
SOURCE_KEY	String	_raw	Specify the KEY to which Splunk software applies REGEX.
CAN_OPTIMIZE	Bool	True	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is needed for the successful evaluation of a search. NOTE: This option should rarely be set to false.
CLEAN_KEYS	Boolean	True	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
FORMAT	String		This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time.

Name	Type	Default	Description	
			This attribute specifies the format of the event, including any field names or values you want to add. FORMAT for index-time extractions: Use $n (for example $1, $2, etc) to specify the output of each REGEX match. If REGEX does not have n groups, the matching fails. The special identifier $0 represents what was in the DEST_KEY before the REGEX was performed. At index-time only, you can use FORMAT to create concatenated fields: FORMAT = ipaddress::$1.$2.$3.$4 When you create concatenated fields with FORMAT, "$" is the only special character. It is treated as a prefix for regex-capturing groups only if it is followed by a number and only if the number applies to an existing capturing group. So if REGEX has only one capturing group and its value is "bar", then: \t"FORMAT = foo$1" yields "foobar" \t"FORMAT = foo$bar" yields "foo$bar" \t"FORMAT = foo$1234" yields "foo$1234" \t"FORMAT = foo$1\\$2" yields "foobar\\$2" At index-time, FORMAT defaults to <stanza-name>::$1 FORMAT for search-time extractions: The format of this field as used during search time extractions is as follows: \tFORMAT = <field-name>::<field-value>(<field-name>::<field-value>)* \tfield-name = [<string>\|$<extracting-group-number>] \tfield-value = [<string>|$<extracting-group-number>] Search-time extraction examples: \tFORMAT = first::$1 second::$2 third::other-value \tFORMAT = $1::$2 You cannot create concatenated fields with FORMAT at search time. That functionality is only available at index time. At search-time, FORMAT defaults to an empty string.	
KEEP_EMPTY_VALS	Boolean		False	If set to true, Splunk software preserves extracted fields with empty values.
MV_ADD	Boolean		False	

Name	Type	Default	Description	
				If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
disabled	Boolean		Specifies whether the field transformation is disabled.	

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: \\tREGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). \\tREGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.

Name	Description
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
disabled	Indicates if the field transformation is disabled.
eai:appName	The Splunk app for which the field extractions are defined. For example, the search app.
eai:userName	The name of the Splunk user who created the field extraction definitions. For example, the admin user.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform -d
REGEX="(?<_KEY_1>[a-z]*),(?<_VAL_1>[a-z]*)" -d SOURCE_KEY=_raw -d CLEAN_KEYS=false
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:33:13-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_transform</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform</id>
    <updated>2011-07-21T20:33:13-07:00</updated>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">0</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX">(?<_KEY_1>[a-z]*),(?<_VAL_1>[a-z]*)</s:key>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/transforms/lookups

`https://<host>:<mPort>/services/data/transforms/lookups`

Access or create lookup definitions.

GET

List lookup definitions.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Datatype	Default	Description
getsize	Boolean	`false`	Enable to return the file size.
replicate_delta	Boolean	`false`	Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	

Name	Description
	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.
GETSIZE	If enabled, returns the file size.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
disabled	Indicates if this lookup is disabled.
eai:appName	The Splunk app for which the lookups are defined. For example, the search app.
eai:userName	The Splunk user for which the lookups are defined.
external_cmd	Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in:

Name	Description
	$SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.
fields_list	List of all fields that are supported by the external command.
replicate_delta	Indicates that only the changes to a CSV lookup table are replicated, rather than the entire lookup table.
type	Specifies the field extraction type. Can be either external or file.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-08-01T21:10:44-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>dnslookup</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/transforms/lookups/dnslookup</id>
    <updated>2011-08-01T21:10:44-07:00</updated>
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup" rel="list"/>
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">1</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX"/>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="external_cmd">external_lookup.py clienthost clientip</s:key>
        <s:key name="fields_list">clienthost clientip</s:key>
        <s:key name="type">external</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update a lookup definition.

Request parameters

Name	Type	Default	Description
collection	String	`<empty>`	Name of the collection to use for this lookup. The collection should be defined in `$SPLUNK_HOME/etc/<app_name>/collections.conf` for the current app. To create a KV Store lookup, use `collection` to pass in the KV Store collection name and include the `external_type` parameter with a value of `kvstore` in your `POST` request.
name	String		The name of the lookup definition.
default_match	String		If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.
disabled	Boolean		Specifies whether the lookup definition is disabled.
external_cmd	String		Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.
external_type	One of the following values: • `python` • `executable` • `geo` • `kvstore`	`python`	Type of external command for performing a lookup. To define a KV Store lookup, use `external_type = kvstore`. Include the KV Store `collection` name in your `POST` request.
fields_list	String		A comma- and space-delimited list of all fields that are supported by the external command. Use this for external (or "scripted") lookups.

Name	Type	Default	Description
filename	String		The name of the static lookup table file.
max_matches	Number		The maximum number of possible matches for each input lookup value.
max_offset_secs	Number		For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.
min_matches	Number		The minimum number of possible matches for each input lookup value.
min_offset_secs	Number		For temporal lookups, this is the minimum time (in seconds) that the event timestamp can be later than the lookup entry timestamp for a match to occur.
replicate_delta	Boolean	`false`	Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.
time_field	String		For temporal lookups, this is the field in the lookup table that represents the timestamp.
time_format	String		For temporal lookups, this specifies the "strptime" format of the timestamp field.

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data.

Name	Description
	This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
default_match	If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.
disabled	Specifies whether the lookup definition is disabled.
eai:appName	The Splunk app for which the lookups are defined. For example, the search app.
eai:userName	The Splunk user for which the lookups are defined.
external_cmd	Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.
fields_list	List of all fields that are supported by the external command. Use this for external (or "scripted") lookups.
filename	The name of the static lookup table file.
max_matches	The maximum number of possible matches for each input lookup value. If the lookup is non-temporal (not time-bounded, meaning the time_field attribute is not specified), Splunk software uses the first <integer> entries, in file order. If the lookup is temporal, Splunk software uses the first <integer> entries in descending time order. Default = 100 if the lookup is not temporal, default = 1 if it is temporal.
max_offset_secs	For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.
min_matches	The minimum number of possible matches for each input lookup value.
min_offset_secs	For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.
time_field	For temporal lookups, this is the field in the lookup table that represents the timestamp.

Name	Description
time_format	For temporal lookups, this specifies the \\"strptime\\" format of the timestamp field.
type	Specifies the field extraction type. Can be either external or file.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups -d
name=my_lookup -d filename=lookup.csv
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-08-01T21:10:33-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup</id>
    <updated>2011-08-01T21:10:33-07:00</updated>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">1</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX"/>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="filename">lookup.csv</s:key>
        <s:key name="type">file</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/transforms/lookups/{name}

`https://<host>:<mPort>/services/data/transforms/lookups/{name}`
Manage the `{name}` lookup definition.

DELETE

Delete a specific lookup definition.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-07-21T20:03:24-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access a specific lookup definition.

Request parameters

Name	Datatype	Default	Description
replicate_delta	Boolean	`false`	Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.

Returned values

Name	Description
CAN_OPTIMIZE	Indicates whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	Indicates whether Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.
KEEP_EMPTY_VALS	Indicates whether Splunk software preserves extracted fields with empty values.
LOOKAHEAD	For index-time filed extractions. Specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	"If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data.

Name	Description
	This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
disabled	Indicates if this lookup is disabled.
eai:appName	The Splunk software app for which the lookups are defined. For example, the search app.
eai:attributes	Field control information.
eai:userName	The Splunk user for which the lookups are defined.
filename	The name of the static lookup table file.
replicate_delta	Indicates that only the changes to a CSV lookup table are replicated, rather than the entire lookup table.
type	Specifies the field extraction type. Can be either external or file.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-08-01T21:11:01-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
  <title>my_lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup</id>
  <updated>2011-08-01T21:11:01-07:00</updated>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="list"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="edit"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="remove"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/move" rel="move"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="CAN_OPTIMIZE">1</s:key>
      <s:key name="CLEAN_KEYS">1</s:key>
      <s:key name="DEFAULT_VALUE"/>
      <s:key name="DEST_KEY"/>
      <s:key name="FORMAT"/>
      <s:key name="KEEP_EMPTY_VALS">0</s:key>
      <s:key name="LOOKAHEAD">4096</s:key>
      <s:key name="MV_ADD">0</s:key>
      <s:key name="REGEX"/>
      <s:key name="SOURCE_KEY">_raw</s:key>
      <s:key name="WRITE_META">0</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl node elided ...
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>default_match</s:item>
              <s:item>disabled</s:item>
              <s:item>external_cmd</s:item>
              <s:item>fields_list</s:item>
              <s:item>filename</s:item>
              <s:item>max_matches</s:item>
              <s:item>max_offset_secs</s:item>
              <s:item>min_matches</s:item>
              <s:item>min_offset_secs</s:item>
              <s:item>replicate_delta</s:item>
              <s:item>time_field</s:item>
              <s:item>time_format</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:userName">admin</s:key>
      <s:key name="filename">lookup.csv</s:key>
      <s:key name="replicate_delta">1</s:key>
      <s:key name="type">file</s:key>
    </s:dict>
  </content>
</entry>
```

```
</feed>
```

POST

Update a lookup definition.

Request parameters

Name	Type	Default	Description
collection	String	`<empty>`	Name of the collection to use for this lookup. The collection should be defined in `$SPLUNK_HOME/etc/<app_name>/collections.conf` for the current app. To create a KV Store lookup, use `collection` to pass in the KV Store collection name and include the `external_type` parameter with a value of `kvstore` in your `POST` request.
default_match	String		If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.
disabled	Boolean		Specifies whether the lookup definition is disabled.
external_cmd	String		Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.
external_type	One of the following values: - `python` - `executable` - `geo` - `kvstore`	`python`	Type of external command for performing a lookup. To define a KV Store lookup, use `external_type = kvstore`. Include the KV Store `collection` name in your `POST` request.
fields_list	String		A comma- and space-delimited list of all fields that are supported by the external command. Use this for external (or "scripted") lookups.
filename	String		The name of the static lookup table file.
max_matches	Number		The maximum number of possible matches for each input lookup value.
max_offset_secs	Number		For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.
min_matches	Number		The minimum number of possible matches for each input lookup value.
min_offset_secs	Number		For temporal lookups, this is the minimum time (in seconds) that the event timestamp can be later than the lookup entry timestamp for a match to occur.
replicate_delta	Boolean	`false`	

Name	Type	Default	Description
			Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.
time_field	String		For temporal lookups, this is the field in the lookup table that represents the timestamp.
time_format	String		For temporal lookups, this specifies the "strptime" format of the timestamp field.

Returned values

Name	Description
CAN_OPTIMIZE	Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are *always* discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.
CLEAN_KEYS	If set to true, Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
DEFAULT_VALUE	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
DEST_KEY	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
FORMAT	This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.
KEEP_EMPTY_VALS	If set to true, Splunk software preserves extracted fields with empty values.
LOOKAHEAD	Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).
MV_ADD	If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.
REGEX	The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.
SOURCE_KEY	The KEY to which Splunk software applies REGEX.
WRITE_META	Indicates whether to automatically write REGEX to metadata.

Name	Description
	This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.
default_match	If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.
disabled	Specifies whether the lookup definition is disabled.
eai:appName	The Splunk app for which the lookups are defined. For example, the search app.
eai:userName	The Splunk user for which the lookups are defined.
external_cmd	Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.
fields_list	List of all fields that are supported by the external command. Use this for external (or "scripted") lookups.
filename	The name of the static lookup table file.
max_matches	The maximum number of possible matches for each input lookup value.
max_offset_secs	For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.
min_matches	The minimum number of possible matches for each input lookup value.
min_offset_secs	For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.
time_field	For temporal lookups, this is the field in the lookup table that represents the timestamp.
time_format	For temporal lookups, this specifies the "strptime" format of the timestamp field.
type	Specifies the field extraction type. Can be either external or file.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup -d
external_cmd=myscript.py -d fields_list=a,b,c
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-07-21T20:00:07-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup</id>
    <updated>2011-07-21T20:00:07-07:00</updated>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="CAN_OPTIMIZE">1</s:key>
        <s:key name="CLEAN_KEYS">1</s:key>
        <s:key name="DEFAULT_VALUE"/>
        <s:key name="DEST_KEY"/>
        <s:key name="FORMAT"/>
        <s:key name="KEEP_EMPTY_VALS">0</s:key>
        <s:key name="LOOKAHEAD">4096</s:key>
        <s:key name="MV_ADD">0</s:key>
        <s:key name="REGEX"/>
        <s:key name="SOURCE_KEY">_raw</s:key>
        <s:key name="WRITE_META">0</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="external_cmd">myscript.py</s:key>
        <s:key name="fields_list">a,b,c</s:key>
        <s:key name="replicate_delta">1</s:key>
        <s:key name="type">external</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/transforms/metric-schema

`https://<host>:<mPort>/services/data/transforms/metric-schema`

Use this endpoint to configure ingest-time log-to-metrics transformations. Identify measurements and blacklist dimensions. Design transformations that target specific event schemas within a log.

Authentication and Authorization

Use of this endpoint is restricted to roles that have the `edit_metric_schema` capability.

Usage Details

For more information about carrying out ingest-time log-to-metrics transformations using this endpoint, see Convert event logs to metric data points in *Metrics*.

GET

List existing log-to-metrics configurations.

Request parameters

None.

Returned parameters

None

Example request and response

XML Request

```
curl -k -u admin:ch@ngeme -X GET
https://localhost:8089/services/data/transforms/metric-schema/splunk_metrics
```

XML Response

```
<title>metric-schema</title>
<id>https://localhost:8089/services/data/transforms/metric-schema</id>
<updated>2018-07-31T17:00:21-07:00</updated>
<generator build="06d0f1f682cc" version="7.1.0"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/data/transforms/metric-schema/_new" rel="create"/>
<link href="/services/data/transforms/metric-schema/_reload" rel="_reload"/>
<link href="/services/data/transforms/metric-schema/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>metric-schema:splunk_metrics</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk
_metrics</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="alternate"/>
<author>
<name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="list"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/_reload"
rel="_reload"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="edit"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
```

```
rel="remove"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/move"
rel="move"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/disable"
rel="disable"/>
<content type="text/xml">
<s:dict>
<s:key name="METRIC-SCHEMA-BLACKLIST-DIMS-queue">location,corp</s:key>
<s:key
name="METRIC-SCHEMA-MEASURES-queue">max_size_kb,current_size_kb,current_size,largest_size,smallest_size</s:key>
<s:key name="disabled">0</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">0</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:key name="removable">1</s:key>
<s:key name="sharing">app</s:key>
</s:dict>
</s:key>
<s:key name="eai:attributes">
<s:dict>
<s:key name="optionalFields">
<s:list>
<s:item>blacklist_dimensions</s:item>
<s:item>field_names</s:item>
<s:item>metric_name_prefix</s:item>
</s:list>
</s:key>
<s:key name="requiredFields">
<s:list/>
</s:key>
<s:key name="wildcardFields">
<s:list/>
</s:key>
</s:dict>
</s:key>
</s:dict>
</content>
</entry>
</feed>
```

POST

Configures ingest-time conversion of log events to metric data points.

Request parameters

Name	Type	Description
name required	String	Required. Name of the `metric-schema` stanza in `transforms.conf`.
field_name required	String	Comma-separated list of measure fields to be extracted from a log line.
blacklist_dimension optional	String	Comma-separated list of dimension fields to be omitted when log events are converted to metric data points.
metric_name_prefix optional	String	Used when the events in a log have more than one schema, meaning that they have differing sets of measure fields and blacklist dimension fields. Takes the value of a field that is shared by all events in the log, and whose values correspond to the different event schemas.

Returned parameters

Name	Type	Description
METRIC-SCHEMA-MEASURES-<metric_name_prefix>	String	Comma-separated list of measure fields to be extracted from a log line.
METRIC-SCHEMA-BLACKLIST-DIMS-<metric_name_prefix>	String	Comma-separated list of dimension fields to be omitted when log events are converted to metric data points.

Example request and response

XML Request

```
curl -k -u admin:ch@ngeme -X POST https://localhost:8089/services/data/transforms/metric-schema -d
"name=splunk_metrics" -d "metric_name_prefix=queue" -d
"field_names=max_size_kb,current_size_kb,current_size,largest_size,smallest_size" -d
"blacklist_dimensions=location,corp"
```

XML Response

```
...
<title>metric-schema</title>
<id>https://localhost:8089/services/data/transforms/metric-schema</id>
<updated>2018-07-31T16:33:54-07:00</updated>
<generator build="06d0f1f682cc" version="7.1.0"/>
<author>
 <name>Splunk</name>
</author>
<link href="/services/data/transforms/metric-schema/_new" rel="create"/>
<link href="/services/data/transforms/metric-schema/_reload" rel="_reload"/>
<link href="/services/data/transforms/metric-schema/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>metric-schema:splunk_metrics</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk
_metrics</id>
```

```
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="list"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/_reload"
rel="_reload"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="edit"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics"
rel="remove"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/move"
rel="move"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/disable"
rel="disable"/>
<content type="text/xml">
 <s:dict>
 <s:key name="METRIC-SCHEMA-BLACKLIST-DIMS-queue">location,corp</s:key>
 <s:key
name="METRIC-SCHEMA-MEASURES-queue">max_size_kb,current_size_kb,current_size,largest_size,smallest_size</s:key>
 <s:key name="disabled">0</s:key>
 <s:key name="eai:acl">
 <s:dict>
 <s:key name="app">search</s:key>
 <s:key name="can_change_perms">1</s:key>
 <s:key name="can_list">1</s:key>
 <s:key name="can_share_app">1</s:key>
 <s:key name="can_share_global">1</s:key>
 <s:key name="can_share_user">0</s:key>
 <s:key name="can_write">1</s:key>
 <s:key name="modifiable">1</s:key>
 <s:key name="owner">nobody</s:key>
  <s:key name="perms">
  <s:dict>
   <s:key name="read">
    <s:list>
      <s:item>*</s:item>
    </s:list>
   </s:key>
   <s:key name="write">
    <s:list>
     <s:item>*</s:item>
    </s:list>
   </s:key>
  </s:dict>
 </s:key>
 <s:key name="removable">1</s:key>
 <s:key name="sharing">app</s:key>
 </s:dict>
 </s:key>
 </s:dict>
</content>
</entry>
</feed>
```

DELETE

Delete existing log-to-metrics configurations.

Request parameters
None.

Returned parameters
None

Example request and response

XML Request

```
curl -k -u admin:ch@ngeme -X DELETE
https://localhost:8089/services/data/transforms/metric-schema/splunk_metrics
```

XML Response

```
<title>metric-schema</title>
<id>https://localhost:8089/services/data/transforms/metric-schema</id>
<updated>2018-07-31T16:56:36-07:00</updated>
<generator build="06d0f1f682cc" version="7.1.0"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/data/transforms/metric-schema/_new" rel="create"/>
<link href="/services/data/transforms/metric-schema/_reload" rel="_reload"/>
<link href="/services/data/transforms/metric-schema/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>
```

data/transforms/statsdextractions

```
https://<host>:<mPort>/services/data/transforms/statsdextractions
```

Use this endpoint to configure dimension extraction from StatsD metrics.

Authentication and Authorization
Use of this endpoint is restricted to roles that have the `edit_statsd_transforms` capability.

Usage Details
For more information about StatsD dimension extraction using this endpoint, see Get metrics in with StatsD in *Metrics*.

POST

Configures dimension extraction from StatsD metrics.

Request parameters

Name	Type	Description

Name	Type	Description
unique_transforms_stanza_name	String	A unique name for this stanza.
REGEX = <regular expression>	String	A regular expression that defines how to match and extract dimensions from StatsD metrics data. Splunk supports a named capturing-group extraction format `(?<diml>group)(?dim2>group) ...` to provide dimension names for the corresponding values that are extracted.
REMOVE_DIMS_FROM_METRIC_NAME= <Boolean>	Boolean	Specifies whether unmatched segments of the StatsD dotted name segment are used as the *metric_name*. When `true`, dimension values are be removed from the measurement and the unmatched portion becomes the *metric_name*. The default value is `true`. When `false`, extracted dimension values are included in the *metric_name*. For example, a metric measurement name is "x.y.z". The regular expression matches "y" and "z". When REMOVE_DIMS_FROM_METRIC_NAME is `true`, *metric_name* is "x". When `false`, *metric_name* is "x.y.z".

Example request and response

Request

```
curl -k -u admin:pass https://localhost:8089/services/data/transforms/statsdextractions \-d
"name=statsd-ex&REGEX=\.(?<hostname>\S%2B?)\.(?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})&REMOVE_DIMS_FROM
_METRIC_NAME=true"
```

Response

```
...
  <title>transforms-statsd</title>
  <id>https://<localhost>:<mport>/services/data/transforms/statsdextractions</id>
  <updated>2017-08-08T23:53:45+00:00</updated>
  <generator build="eb729684699b" version="7.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/transforms/statsdextractions/_new" rel="create"/>
  <link href="/services/data/transforms/statsdextractions/_reload" rel="_reload"/>
  <link href="/services/data/transforms/statsdextractions/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>statsd-dims:statsd-ex</title>
    <id>https://epic-metriks-splk.sv.splunk.com:8089/servicesNS/nobody/search/data/transforms
/statsdextractions/statsd-dims%3Astatsd-ex</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex"
rel="list"/>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex"
rel="edit"/>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex"
rel="remove"/>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex/move"
rel="move"/>
    <link href="/servicesNS/nobody/search/data/transforms/statsdextractions/statsd-dims%3Astatsd-ex/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="REGEX">\.(?<hostname>\S+?)\.(?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})</s:key>
        <s:key name="REMOVE_DIMS_FROM_METRIC_NAME">1</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">0</s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_share_app">0</s:key>
            <s:key name="can_share_global">0</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/ui/global-banner

`https://<host>:<mPort>/services/data/ui/global-banner`

View or create a global banner.

Authentication and Authorization

Use of the POST function of this endpoint is restricted to users with an `edit_global_banner` capability. The GET function of this endpoint is not restricted.

GET

View a global banner.

Request parameters

None.

Returned values

Name	Description
background_color	Indicates the color of the banner.
hyperlink	The link included in the banner.
hyperlink_text	Display text for the link in the banner.
message	Banner notification text.
visible	Boolean value indicating whether the banner is visible.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON
```

XML Response

```
...
  <entry>
    <title>BANNER_MESSAGE_SINGLETON</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON" rel="list"/>
    <link href="/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>global_banner.background_color</s:item>
                <s:item>global_banner.hyperlink</s:item>
                <s:item>global_banner.hyperlink_text</s:item>
                <s:item>global_banner.message</s:item>
                <s:item>global_banner.visible</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="global_banner.background_color">red</s:key>
        <s:key name="global_banner.hyperlink"></s:key>
        <s:key name="global_banner.hyperlink_text"></s:key>
        <s:key name="global_banner.message">Server maintenance from 2am-6am</s:key>
        <s:key name="global_banner.visible">1</s:key>
      </s:dict>
    </content>
  </entry>
...
```

POST

Create a new global banner.

Request parameters

Name	Type	Default	Description
background_color required	String	blue	Indicates the color of the banner. The color can be any of the following: • green • blue • yellow • orange • red
hyperlink optional	String		The link included in the banner. The link must begin with `http://`or `https://`.
hyperlink_text optional	String		Display text for the link in the banner.
message required	String	*sample text*	Banner notification text.
visible required	Boolean	false	Indicates whether the banner is visible.

Returned values

Name	Description
background_color	Indicates the color of the banner.
hyperlink	The link included in the banner.
hyperlink_text	Display text for the link in the banner.
message	Banner notification text.
visible	Boolean value indicating whether the banner is visible.

Example request and response

XML Request

```
curl -X POST -k -u admin:pass
https://localhost:8089/servicesNS/nobody/system/data/ui/global-banner/BANNER_MESSAGE_SINGLETON -d
global_banner.message="example banner message"
```

XML Response

```
...
  <entry>
    <title>BANNER_MESSAGE_SINGLETON</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/ui/global-banner/BANNER_MESSAGE_SINGLETON</id>
    <updated>2020-04-02T16:39:12-07:00</updated>
    <link href="/servicesNS/admin/search/data/ui/global-banner/BANNER_MESSAGE_SINGLETON" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/ui/global-banner/BANNER_MESSAGE_SINGLETON" rel="list"/>
    <link href="/servicesNS/admin/search/data/ui/global-banner/BANNER_MESSAGE_SINGLETON/_reload"
```

```
rel="_reload"/>
    <link href="/servicesNS/admin/search/data/ui/global-banner/BANNER_MESSAGE_SINGLETON" rel="edit"/>
    <link href="/servicesNS/admin/search/data/ui/global-banner/BANNER_MESSAGE_SINGLETON/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="global_banner.background_color">red</s:key>
        <s:key name="global_banner.hyperlink"></s:key>
        <s:key name="global_banner.hyperlink_text"></s:key>
        <s:key name="global_banner.message">example banner message</s:key>
        <s:key name="global_banner.visible">1</s:key>
      </s:dict>
    </content>
  </entry>
...
```

data/ui/panels

`https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/panels`

View, add, or edit dashboard panels.

GET

Access all the XML definitions for existing panels.

Request parameters

None.

Returned values

Name	Description
eai:appName	App context for the panel.
eai:data	XML definition for the panel.

Name	Description
eai:userName	User who created the panel.
label	Panel label.
panel.title	Panel title.
rootNode	XML root node.

Example request and response

XML Request

```
curl --get -k -u username:password
https://localhost:8089/servicesNS/admin/search/data/ui/panels
```

XML Response

```
<title>panels</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/panels</id>
  <updated>2018-12-17T12:03:14-08:00</updated>
  <generator build="8f0ead9ec3db" version="7.1.1"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/panels/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/ui/panels/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/panels/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>new_panel</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/ui/panels/new_panel</id>
    <updated>2018-12-17T12:02:57-08:00</updated>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="list"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="edit"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="remove"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:data"><![CDATA[<panel><label>the_new_label</label></panel>]]></s:key>
        <s:key name="eai:digest">1c70628bb4aeec0470707e59e1b2d321</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="label">the_new_label</s:key>
        <s:key name="panel.title">new_panel</s:key>
        <s:key name="rootNode">panel</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create a new dashboard panel source XML definition.

Request parameters

Name	Type	Default	Description
name	String		Panel name.
eai:data	XML document		Panel XML definition.

Returned values

Name	Description
eai:appName	App context for the panel.
eai:data	XML definition for the panel.
eai:userName	User who created the panel.
label	Panel label.
panel.title	Panel title.
rootNode	XML root node.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/ui/panels -d
"name=new_panel&eai:data=<panel><label>the_new_label</label></panel>"
```

XML Response

```
<title>panels</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/panels</id>
  <updated>2018-12-17T12:02:57-08:00</updated>
  <generator build="8f0ead9ec3db" version="7.1.1"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/panels/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/ui/panels/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/panels/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>new_panel</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/ui/panels/new_panel</id>
    <updated>2018-12-17T12:02:57-08:00</updated>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="list"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="edit"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="remove"/>
    <link href="/servicesNS/admin/search/data/ui/panels/new_panel/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:data"><![CDATA[<panel><label>the_new_label</label></panel>]]></s:key>
        <s:key name="eai:digest">1c70628bb4aeec0470707e59e1b2d321</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="label">the_new_label</s:key>
        <s:key name="panel.title">new_panel</s:key>
        <s:key name="rootNode">panel</s:key>
      </s:dict>
    </content>
  </entry>
```

data/ui/views

`https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/views`

View or create a dashboard source XML definition.

GET

Access all the XML definitions for existing dashboards.

Request parameters

None.

Returned values

Name	Description
eai:appName	App context for the dashboard.
eai:data	XML definition for the dashboard.
eai:type	User interface type. For dashboards, this type is `view`.
eai:userName	User who created the dashboard.
isDashboard	Boolean value indicating whether the knowledge object is a dashboard.
isVisible	Boolean value indicating whether the dashboard is visible.
label	Dashboard label.
rootNode	XML root node.

Example request and response

XML Request

```
curl --get -k -u username:password
https://localhost:8089/servicesNS/admin/search/data/ui/views
```

XML Response

```
<title>views</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
  <updated>2015-10-08T16:17:03-07:00</updated>
  <generator build="a1c9b18fdcfc" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/views/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/ui/views/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/views/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
```

```
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title> my_dashboard </title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard</id>
  <updated>2015-10-08T16:17:03-07:00</updated>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="list"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="edit"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="remove"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard/move" rel="move"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms"/>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">user</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>eai:type</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list>
              <s:item>eai:data</s:item>
            </s:list>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:data"><![CDATA[<dashboard><label>my_dashboard_label</label></dashboard>]]></s:key>
      <s:key name="eai:digest">01778119e0d9352ca0c6eb0aa7f00950</s:key>
      <s:key name="eai:type">views</s:key>
      <s:key name="eai:userName">admin</s:key>
      <s:key name="isDashboard">1</s:key>
      <s:key name="isVisible">1</s:key>
      <s:key name="label">my_dashboard_label</s:key>
      <s:key name="rootNode">dashboard</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Create a new dashboard source XML definition.

Request parameters

Name	Type	Default	Description
name	String		Dashboard name.
eai:data	XML document		Dashboard XML definition.

Returned values

Name	Description
eai:appName	App context for the dashboard.
eai:data	XML definition for the dashboard.
eai:type	User interface type. For dashboards, this type is `view`.
eai:userName	User who created the dashboard.
isDashboard	Boolean value indicating whether the knowledge object is a dashboard.
isVisible	Boolean value indicating whether the dashboard is visible.
label	Dashboard label.
rootNode	XML root node.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/ui/views -d
"name=new_dashboard&eai:data=<dashboard><label>the_new_label</label></dashboard>"
```

XML Response

```
<title>views</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
  <updated>2015-10-08T15:50:01-07:00</updated>
  <generator build="a1c9b18fdcfc" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/views/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/ui/views/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/views/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>new_dashboard</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/ui/views/new_dashboard</id>
    <updated>2015-10-08T15:50:01-07:00</updated>
    <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="list"/>
    <link href="/servicesNS/admin/search/data/ui/views/new_dashboard/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="edit"/>
    <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="remove"/>
    <link href="/servicesNS/admin/search/data/ui/views/new_dashboard/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:data"><![CDATA[<dashboard><label> the_new_label </label></dashboard>]]></s:key>
        <s:key name="eai:digest">533c60e648b7c4733321ae205d2627d8</s:key>
        <s:key name="eai:type">views</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="isDashboard">1</s:key>
        <s:key name="isVisible">1</s:key>
        <s:key name="label">the_new_label</s:key>
        <s:key name="rootNode">dashboard</s:key>
      </s:dict>
    </content>
  </entry>
```

data/ui/views/{name}

`https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/views/{name}`

Access or update source XML for an existing dashboard.

GET

Access an existing dashboard XML definition.

Request parameters

None.

Returned values

Name	Description
eai:appName	App context for the dashboard.
eai:data	XML definition for the dashboard.
eai:type	User interface type. For dashboards, this type is `view`.
eai:userName	User who created the dashboard.
isDashboard	Boolean value indicating whether the knowledge object is a dashboard.
isVisible	Boolean value indicating whether the dashboard is visible.
label	Dashboard label.
rootNode	XML root node.

Example request and response

XML Request

```
curl -k -u username:password
https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard
```

XML Response

```
<title>views</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
  <updated>2015-10-08T16:17:03-07:00</updated>
  <generator build="a1c9b18fdcfc" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/views/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/ui/views/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/views/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title> my_dashboard </title>
    <id>https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard</id>
    <updated>2015-10-08T16:17:03-07:00</updated>
    <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="list"/>
    <link href="/servicesNS/admin/search/data/ui/views/my_dashboard/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="edit"/>
    <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="remove"/>
    <link href="/servicesNS/admin/search/data/ui/views/my_dashboard/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>eai:type</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>eai:data</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:data"><![CDATA[<dashboard><label>my_dashboard_label</label></dashboard>]]></s:key>
        <s:key name="eai:digest">01778119e0d9352ca0c6eb0aa7f00950</s:key>
        <s:key name="eai:type">views</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="isDashboard">1</s:key>
        <s:key name="isVisible">1</s:key>
        <s:key name="label">my_dashboard_label</s:key>
        <s:key name="rootNode">dashboard</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update a specific dashboard XML definition.

Request parameters

Name	Type	Default	Description
eai:changelog optional	string		Enables to specify a revision message when modifying a dashboard. The message appears in the response from the `data/ui/views/{name}/history` endpoint.
eai:data	XML document		Dashboard XML definition.

Returned values

Name	Description
eai:appName	App context for the dashboard.
eai:data	XML definition for the dashboard.
eai:type	User interface type. For dashboards, this type is `view`.
eai:userName	User who created the dashboard.
isDashboard	Boolean value indicating whether the knowledge object is a dashboard.
isVisible	Boolean value indicating whether the dashboard is visible.
label	Dashboard label.
rootNode	XML root node.

Example request and response

JSON Request

```
curl -X POST -u username:password -k
"https://localhost:8106/servicesNS/admin/search/data/ui/views/my_dashboard?output_mode=json" \
> -d eai:data="<dashboard><label>new label</label></dashboard>" \
> -d eai:changelog="Second version"
```

JSON Response

```
  {
    "links": {
        "create": "/servicesNS/admin/search/data/ui/views/_new",
        "_reload": "/servicesNS/admin/search/data/ui/views/_reload",
        "_acl": "/servicesNS/admin/search/data/ui/views/_acl"
    },
    "origin": "https://localhost:8106/servicesNS/admin/search/data/ui/views",
    "updated": "2024-09-09T02:54:23-07:00",
    "generator": {
        "build": "b0122e4d425e5c0d37a7278576a02b962b3505f7",
        "version": "20240906"
    },
    "entry": [
        {
            "name": "new_dashboard_from_rest_api",
            "id":
"https://localhost:8106/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api",
            "updated": "2024-09-09T02:54:23-07:00",
            "links": {
                "alternate": "/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api",
                "list": "/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api",
                "_reload": "/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api/_reload",
                "edit": "/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api",
                "remove": "/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api",
                "move": "/servicesNS/admin/search/data/ui/views/new_dashboard_from_rest_api/move"
            },
            "author": "admin",
            "acl": {
                "app": "search",
                "can_change_perms": true,
                "can_list": true,
                "can_share_app": true,
                "can_share_global": true,
                "can_share_user": true,
                "can_write": true,
                "modifiable": true,
                "owner": "admin",
                "perms": null,
                "removable": true,
                "sharing": "user"
            },
            "content": {
                "disabled": false,
                "eai:acl": null,
                "eai:appName": "search",
                "eai:data": "<dashboard><label>new label</label></dashboard>",
                "eai:digest": "7ae3fd31bfc2387a3ab8e1e2244f44ce",
                "eai:type": "views",
                "eai:userName": "admin",
                "isDashboard": true,
                "isVisible": true,
                "label": "new label",
                "rootNode": "dashboard",
                "version": ""
            }
        }
    ],
    "paging": {
        "total": 1,
        "perPage": 30,
        "offset": 0
    },
    "messages": []
}
```

DELETE

Delete a specific dashboard.

Request parameters

Name	Type	Default	Description
eai:changelog optional	string		Enables to specify a message when deleting a dashboard.

Returned values
None.

Example request and response

JSON Request

```
curl -X DELETE -u username:password -k
"https://localhost:8106/servicesNS/admin/search/data/ui/views/my_dashboard?output_mode=json" \

> -d eai:changelog="Removed as agreed on Sep. 15"
```

JSON Response

```
{
    "links": {
        "create": "/servicesNS/admin/search/data/ui/views/_new",
        "_reload": "/servicesNS/admin/search/data/ui/views/_reload",
        "_acl": "/servicesNS/admin/search/data/ui/views/_acl"
    },
    "origin": "https://localhost:8106/servicesNS/admin/search/data/ui/views",
    "updated": "2024-09-09T02:59:04-07:00",
    "generator": {
        "build": "b0122e4d425e5c0d37a7278576a02b962b3505f7",
        "version": "20240906"
    },
    "entry": [],
    "paging": {
        "total": 0,
        "perPage": 30,
        "offset": 0
    },
    "messages": []
}
```

data/ui/views/{name}/history

```
https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/views/{name}/history?output_mode=json"
```

View the revision history of a {name} dashboard.

GET

Access revisions made to a {name} dashboard.

Request parameters

Name	Type	Default	Description
with_message optional	String		Enable to return the revisions with a non-empty commit message. .

Example request and response

JSON Request

```
curl -X GET -u admin:changeme -k
"https://localhost:8106/servicesNS/admin/search//data/ui/views/my_dashboard/history?output_mode=json"
```

JSON Response

```
{
    "links": {
        "create": "/servicesNS/admin/search/data/ui/views/_new",
        "_reload": "/servicesNS/admin/search/data/ui/views/_reload",
        "_acl": "/servicesNS/admin/search/data/ui/views/_acl"
    },
    "origin": "https://localhost:8106/servicesNS/admin/search/data/ui/views",
    "updated": "2024-09-09T02:42:12-07:00",
    "generator": {
        "build": "b0122e4d425e5c0d37a7278576a02b962b3505f7",
        "version": "20240906"
    },
    "entry": [
        {
            "name": "0000000",
            "id": "https://localhost:8106/servicesNS/admin/search/data/ui/views/0000000",
            "updated": "1969-12-31T16:00:00-08:00",
            "links": {
                "alternate": "/servicesNS/admin/search/data/ui/views/0000000",
                "list": "/servicesNS/admin/search/data/ui/views/0000000",
                "_reload": "/servicesNS/admin/search/data/ui/views/0000000/_reload",
                "edit": "/servicesNS/admin/search/data/ui/views/0000000",
                "remove": "/servicesNS/admin/search/data/ui/views/0000000",
                "move": "/servicesNS/admin/search/data/ui/views/0000000/move"
            },
            "author": "system",
            "acl": {
                "app": "",
                "can_list": true,
                "can_write": true,
                "modifiable": false,
                "owner": "system",
                "perms": {
                    "read": [
                        "*"
                    ],
                    "write": [
                        "*"
                    ]
                },
                "removable": false,
                "sharing": "system"
            },
            "content": {
                "eai:acl": null,
                "email": "admin",
                "message": "Adding a simple pie chart\nto what we discussed today\nduring our team meeting
with the whole team.",
                "sha": "b1e95cd497095b428ebcf40ea6667e0dc9fb1634",
                "time": "2024-09-06T09:59:46+00:00",
                "user": "admin"
            }
        },
        {
            "name": "0000001",
            "id": "https://localhost:8106/servicesNS/admin/search/data/ui/views/0000001",
            "updated": "1969-12-31T16:00:00-08:00",
            "links": {
                "alternate": "/servicesNS/admin/search/data/ui/views/0000001",
                "list": "/servicesNS/admin/search/data/ui/views/0000001",
                "_reload": "/servicesNS/admin/search/data/ui/views/0000001/_reload",
                "edit": "/servicesNS/admin/search/data/ui/views/0000001",
                "remove": "/servicesNS/admin/search/data/ui/views/0000001",
                "move": "/servicesNS/admin/search/data/ui/views/0000001/move"
            },
            "author": "system",
            "acl": {
                "app": "",
                "can_list": true,
                "can_write": true,
                "modifiable": false,
                "owner": "system",
                "perms": {
                    "read": [
                        "*"
                    ],
                    "write": [
                        "*"
                    ]
                },
                "removable": false,
                "sharing": "system"
            },
            "content": {
                "eai:acl": null,
                "email": "admin",
                "message": "Adding chart",
                "sha": "2e5ec14d8c59e466eb019836f494dc86e3a6b34f",
                "time": "2024-09-06T09:58:20+00:00",
                "user": "admin"
            }
        },
        {
            "name": "0000002",
            "id": "https://localhost:8106/servicesNS/admin/search/data/ui/views/0000002",
            "updated": "1969-12-31T16:00:00-08:00",
            "links": {
                "alternate": "/servicesNS/admin/search/data/ui/views/0000002",
                "list": "/servicesNS/admin/search/data/ui/views/0000002",
                "_reload": "/servicesNS/admin/search/data/ui/views/0000002/_reload",
                "edit": "/servicesNS/admin/search/data/ui/views/0000002",
                "remove": "/servicesNS/admin/search/data/ui/views/0000002",
                "move": "/servicesNS/admin/search/data/ui/views/0000002/move"
            },
            "author": "system",
            "acl": {
                "app": "",
                "can_list": true,
                "can_write": true,
                "modifiable": false,
                "owner": "system",
                "perms": {
                    "read": [
                        "*"
                    ],
                    "write": [
                        "*"
                    ]
                },
                "removable": false,
                "sharing": "system"
            },
            "content": {
                "eai:acl": null,
                "email": "admin",
                "message": "",
                "sha": "5f049c0d58bde449cacf72e5a5d282525b6f20d5",
                "time": "2024-09-06T09:57:26+00:00",
                "user": "admin"
            }
        }
    ],
    "paging": {
        "total": 3,
        "perPage": 30,
        "offset": 0
    },
    "messages": []
}
```

data/ui/views/{name}/revision

```
https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/views/{name}/revision?output_mode=json" -d
{revision_id}
```

View a specific revision of a {name} dashboard.

GET

Access a specific revision made to a {name} dashboard.

Request parameters

Name	Type	Default	Description
revision_id required	String		A SHA hash value returned in response from the `data/ui/views/{name}` endpoint. .

Example request and response

JSON Request

```
curl -X GET -u admin:changeme -k
"https://localhost:8106/servicesNS/admin/search/data/ui/views/my_dashboard/revision?output_mode=json" -d
```

```
revision_id=2e5ec14d8c59e466eb019836f494dc86e3a6b34f"
```

JSON Response

```
{
    "links": {
        "create": "/servicesNS/admin/search/data/ui/views/_new",
        "_reload": "/servicesNS/admin/search/data/ui/views/_reload",
        "_acl": "/servicesNS/admin/search/data/ui/views/_acl"
    },
    "origin": "https://localhost:8106/servicesNS/admin/search/data/ui/views",
    "updated": "2024-09-09T02:39:43-07:00",
    "generator": {
        "build": "b0122e4d425e5c0d37a7278576a02b962b3505f7",
        "version": "20240906"
    },
    "entry": [
        {
            "name": "revision",
            "id": "https://localhost:8106/servicesNS/admin/search/data/ui/views/revision",
            "updated": "1969-12-31T16:00:00-08:00",
            "links": {
                "alternate": "/servicesNS/admin/search/data/ui/views/revision",
                "list": "/servicesNS/admin/search/data/ui/views/revision",
                "_reload": "/servicesNS/admin/search/data/ui/views/revision/_reload",
                "edit": "/servicesNS/admin/search/data/ui/views/revision",
                "remove": "/servicesNS/admin/search/data/ui/views/revision",
                "move": "/servicesNS/admin/search/data/ui/views/revision/move"
            },
            "author": "system",
            "acl": {
                "app": "",
                "can_list": true,
                "can_write": true,
                "modifiable": false,
                "owner": "system",
                "perms": {
                    "read": [
                        "*"
                    ],
                    "write": [
                        "*"
                    ]
                },
                "removable": false,
                "sharing": "system"
            },
            "content": {
                "eai:acl": null,
                "eai:data": "\n<dashboard version=\"2\" theme=\"light\">\n    <label>my_dashboard</label>\n
   <description></description>\n    <definition><![CDATA[\n{\n\t\"visualizations\":
{\n\t\t\"viz_DqjYhNwU\": {\n\t\t\t\"type\": \"splunk.line\",\n\t\t\t\"options\":
{}\n\t\t},\n\t\t\"viz_fapFXy0Y\": {\n\t\t\t\"type\": \"splunk.bar\",\n\t\t\t\"options\":
{}\n\t\t}\n\t},\n\t\"dataSources\": {},\n\t\"defaults\": {\n\t\t\"dataSources\": {\n\t\t\t\"ds.search\":
{\n\t\t\t\t\"options\": {\n\t\t\t\t\t\"queryParameters\": {\n\t\t\t\t\t\t\"latest\":
\"$global_time.latest$\",\n\t\t\t\t\t\t\"earliest\":
\"$global_time.earliest$\"\n\t\t\t\t\t}\n\t\t\t\t}\n\t\t\t}\n\t\t}\n\t},\n\t\"inputs\":
{\n\t\t\"input_global_trp\": {\n\t\t\t\"type\": \"input.timerange\",\n\t\t\t\"options\":
{\n\t\t\t\t\"token\": \"global_time\",\n\t\t\t\t\"defaultValue\":
\"-24h@h,now\"\n\t\t\t},\n\t\t\t\"title\": \"Global Time Range\"\n\t\t}\n\t},\n\t\"layout\":
{\n\t\t\"options\": {},\n\t\t\"globalInputs\": [\n\t\t\t\"input_global_trp\"\n\t\t],\n\t\t\"tabs\":
```

```
{\n\t\t\t\"items\": [\n\t\t\t\t{\n\t\t\t\t\t\"layoutId\": \"layout_1\",\n\t\t\t\t\t\"label\": \"New
tab\"\n\t\t\t\t}\n\t\t\t]\n\t\t},\n\t\t\"layoutDefinitions\": {\n\t\t\t\"layout_1\": {\n\t\t\t\t\"type\":
\"absolute\",\n\t\t\t\t\"structure\": [\n\t\t\t\t\t{\n\t\t\t\t\t\t\"item\":
\"viz_DqjYhNwU\",\n\t\t\t\t\t\t\"type\": \"block\",\n\t\t\t\t\t\t\"position\": {\n\t\t\t\t\t\t\t\"x\":
0,\n\t\t\t\t\t\t\t\"y\": 0,\n\t\t\t\t\t\t\t\"w\": 300,\n\t\t\t\t\t\t\t\"h\":
300\n\t\t\t\t\t\t}\n\t\t\t\t\t},\n\t\t\t\t\t{\n\t\t\t\t\t\t\"item\":
\"viz_fapFXy0Y\",\n\t\t\t\t\t\t\"type\": \"block\",\n\t\t\t\t\t\t\"position\": {\n\t\t\t\t\t\t\t\"x\":
300,\n\t\t\t\t\t\t\t\"y\": 0,\n\t\t\t\t\t\t\t\"w\": 300,\n\t\t\t\t\t\t\t\"h\":
300\n\t\t\t\t\t\t}\n\t\t\t\t\t}\n\t\t\t\t],\n\t\t\t\t\"options\": {\n\t\t\t\t\t\"width\":
1440,\n\t\t\t\t\t\"height\": 960,\n\t\t\t\t\t\"display\":
\"auto\"\n\t\t\t\t}\n\t\t\t}\n\t\t}\n\t},\n\t\"description\": \"\",\n\t\"title\": \"my_dashboard\"\n}\n
   ]]></definition>\n    <meta type=\"hiddenElements\"><![CDATA[\n{\n\t\"hideEdit\":
false,\n\t\"hideOpenInSearch\": false,\n\t\"hideExport\": false\n}\n    ]]></meta>\n</dashboard>",
                "email": "admin",
                "message": "Adding chart",
                "sha": "2e5ec14d8c59e466eb019836f494dc86e3a6b34f",
                "time": "2024-09-06T09:58:20+00:00",
                "user": "admin"
            }
        }
    ],
    "paging": {
        "total": 1,
        "perPage": 30,
        "offset": 0
    },
    "messages": []
}
```

datamodel/acceleration (DEPRECATED)

`https://<host>:<mPort>/services/datamodel/acceleration`

Access information about data models that have acceleration enabled.

datamodel/acceleration/{name} (DEPRECATED)

`https://<host>:<mPort>/services/datamodel/acceleration/{name}`

Get information about the `{name}` datamodel.

Note: This endpoint is deprecated.

GET

Get information about a specific data model.

Request parameters
None

Returned values

Name	Description
acceleration	Indicates if acceleration is enabled for this data model.
acceleration.earliest_time	The earliest time to dispatch the search.
search	Specifies the search to accelerate this data model.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/acceleration/simpleMyAppModel
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/acceleration</id>
  <updated>2013-08-24T12:55:07-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>simpleMyAppModel</title>
    <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/acceleration
/simpleMyAppModel</id>
    <updated>2013-08-24T12:55:07-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/acceleration/simpleMyAppModel" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/acceleration/simpleMyAppModel" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">1</s:key>
        <s:key name="acceleration.earliest_time">-1mon</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:digest">9a9dba7c96b3f81554e3773b8d8fe45e</s:key>
        <s:key name="eai:type">datamodels</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="search"><![CDATA[uri=*  status=*  clientip=*  referer=*  useragent=*
 (sourcetype=access_*)  (status < 600)  |
        . . . elided . . .
        "HTTP_Request.HTTP_Success.is_not_Pageview", "HTTP_Request.HTTP_Success.Pageview.myevalfield2"]]>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

datamodel/model

`https://<host>:<mPort>/services/datamodel/model`

Access or create data models.

GET

List data models on the server.

Request parameters

Name	Type	Default	Description
concise	Boolean		Indicates whether to list a concise JSON description of the data model. The concise description is a summary for human readability. It is not used to create the data model.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
acceleration	Indicates whether acceleration is enabled for the data model.
concise	Indicates whether to list a concise JSON description of the data model.
description	The JSON describing the data model.
displayName	The name displayed for the data model in Splunk Web.
eai:appName	The Splunk app in which the data model was created.

Name	Description
eai:userName	The name of the user who created the data model.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/model
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-15T11:42:06-07:00</updated>
  <generator build="176231" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>MyApp</title>
    <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/model/MyApp</id>
    <updated>2013-08-23T15:03:13-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="list"/>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">{"enabled": false}</s:key>
        <s:key name="description"><![CDATA[{"objects": [{"lineage": "HTTP_Request", "previewSearch": " |
search  (sourcetype=access_* OR sourcetype=iis*)
        . . . elided . . .
         "modelName": "MyApp", "displayName": "Web Intelligence"}]]>
        </s:key>
        <s:key name="displayName">Web Intelligence</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
```

```
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>power</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:digest">b8ebd9315dddf8a5e572187f57ddc9de</s:key>
        <s:key name="eai:type">models</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
  . . . elided . . .
</feed>
```

POST

Create a new data model.

Request parameters

Name	Type	Default	Description
description	String		JSON description of the data model.
name	String		Name of the data model.

acceleration	String		Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.
			• *enabled* (true or false)
			• *earliest_time* (time modifier)
			• *cron_schedule* (cron string)
			Example
			`acceleration= ' {`
			`    "enabled": true,`
			`    "earliest_time": -1mon,`
			`    "cron_schedule": 0 */12 * * *`
			`    } '`

Name	Type	Default	Description

Hunk data model acceleration settings	See description		Use these settings to configure acceleration for Hunk data models.
			• *hunk.compression_codec*
			String, case-sensitive.
			Specifies the compression codec to be used for the accelerated orc or parquet format files.
			For `parquet` file format, use `snappy` or `gzip`.
			For `orc` file format, use `snappy` or `zlib`.
			• *hunk.dfs_block_size*
			Unsigned integer
			Specifies the block size in bytes for the compression files.
			• *hunk.file_format*
			String, case sensitive.
			Valid options are `orc` and `parquet`
			Example
			`acceleration= ' {`
			`    "hunk.file_format": "orc",`
			`    "hunk.compression_codec": "snappy"`
			`    } '`

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/model -d name=Debugger --data-urlencode
description='{"modelName":"Debugger","displayName":"Debugger", "description": "A data model for debugging
purposes". . . elided . . . }'
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://qa-sv-rh61x64-10:8089/services/datamodel/model</id>
  <updated>2013-10-16T11:19:24-07:00</updated>
  <generator build="183095" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Debugger</title>
    <id>https://qa-sv-rh61x64-10:8089/servicesNS/admin/search/datamodel/model/Debugger</id>
    <updated>2013-10-16T11:19:24-07:00</updated>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="list"/>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="edit"/>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">{"enabled": false}</s:key>
        <s:key name="description">
          <![CDATA[{"displayName": "Debugger", "modelName": "Debugger", "objectSummary": \
        ...
        "autoextractSearch": " (index = _internal) "}]}]]>
        </s:key>
        <s:key name="displayName">Debugger</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          {'optionalFields': ['acceleration', 'acceleration.cron_schedule', \
           'acceleration.earliest_time', 'eai:data'], 'requiredFields': [], 'wildcardFields': []}
        </s:key>
        <s:key name="eai:digest">05ca1a193365a3b613b919c6401591e3</s:key>
        <s:key name="eai:type">models</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

datamodel/model/{name}

`https://<host>:<mPort>/services/datamodel/model/{name}`

Access, delete, or update the `{name}` data model.

DELETE

Delete a specific data model.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/services/datamodel/model/MyApp
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-24T15:00:54-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

GET

Access a specific data model.

Request parameters

Name	Type	Default	Description
concise	Boolean		Indicates whether to list a concise JSON description of the data model. The concise description is a summary for human readability. It is not used to create the data model.

Returned values

Name	Description
acceleration	Indicates whether acceleration is enabled for the data model.

Name	Description
concise	Indicates whether to list a concise JSON description of the data model.
description	The JSON describing the data model.
displayName	The name displayed for the data model in Splunk Web.
eai:appName	The Splunk app in which the data model was created.
eai:attributes	Field control information.
eai:userName	The name of the Splunk user who created the data model.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/model/MyApp
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-24T13:07:36-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>MyApp</title>
    <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/model/MyApp</id>
    <updated>2013-08-24T13:07:36-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="list"/>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">{"enabled": false}</s:key>
        <s:key name="description"><![CDATA[{"modelName": "MyApp", "objectNameList": ["HTTP_Request",
"ApacheAccessSearch", "IISAccessSearch",
        . . . elided . . .
        "Interface Implementations": 0, "Search-Based": 1}, "description": "Data model for web analytics.",
"displayName": "Web Intelligence"}]]>
        </s:key>
        <s:key name="displayName">Web Intelligence</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>acceleration</s:item>
                <s:item>concise</s:item>
                <s:item>description</s:item>
                <s:item>provisional</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:digest">b8ebd9315dddf8a5e572187f57ddc9de</s:key>
        <s:key name="eai:type">models</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update a specific data model.

Request parameters

Name	Type	Default	Description

acceleration	String		Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.
			• *enabled* (true or false)
			• *earliest_time* (time modifier)
			• *cron_schedule* (cron string)
			Example
			`acceleration= ' {`
			`    "enabled": true,`
			`    "earliest_time": -1mon,`
			`    "cron_schedule": 0 */12 * * *`
			`    } '`

Hunk data model acceleration settings	See description		Use these settings to configure acceleration for Hunk data models.

Name	Type	Default	Description

			• *hunk.compression_codec*
			String, case-sensitive.
			Specifies the compression codec to be used for the accelerated orc or parquet format files.
			For `parquet` file format, use `snappy` or `gzip`.
			For `orc` file format, use `snappy` or `zlib`.
			• *hunk.dfs_block_size*
			Unsigned integer
			Specifies the block size in bytes for the compression files.
			• *hunk.file_format*
			String, case sensitive.
			Valid options are `orc` and `parquet`
			Example
			`acceleration= ' {`
			`    "hunk.file_format": "orc",`
			`    "hunk.compression_codec": "snappy"`
			`    } '`

description	String		JSON description of the data model.
provisional	Boolean		Indicates whether the data model is provisional. Provisional data models are not saved. Specify true to validate a data model before saving it. If the endpoint returns with no errors, then specify this endpoint again, with provisional set to false, to save the data model.

Returned values

Name	Description
acceleration	Indicates whether acceleration is enabled for the data model.
concise	Indicates whether to list a concise JSON description of the data model.
description	The JSON describing the data model.
displayName	The name displayed for the data model in Splunk Web.
eai:appName	The Splunk app in which the data model was created.
eai:attributes	Field control information.
eai:userName	The name of the Splunk user who created the data model.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/model/MyApp -d concise=true
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-24T13:35:54-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>MyApp</title>
    <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/model/MyApp</id>
    <updated>2013-08-24T13:35:54-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="list"/>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">{"enabled": false, "earliest_time": "-1mon"}</s:key>
        <s:key name="description"><![CDATA[{"modelName": "MyApp", "objects": [{"constraints": [{"search":
"sourcetype=access_* OR
        . . . elided . . .
        "PodcastDownload", "WebSession", "User"], "description": "Data model for web analytics."}]]>
        </s:key>
        <s:key name="displayName">Web Intelligence</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">{'wildcardFields': [], 'requiredFields': [], 'optionalFields':
['acceleration', 'acceleration.cron_schedule', 'acceleration.earliest_time', 'eai:data']}</s:key>
        <s:key name="eai:digest">d73ff2d833e3104eed99a8fd258dbae1</s:key>
        <s:key name="eai:type">datamodels</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

datamodel/pivot

`https://<host>:<mPort>/services/datamodel/pivot/{name}`

Access pivots that are based on named data models.

GET

Get information about a specific pivot.

Usage details

`{name}` refers to a data model on the system.

Specify a pivot using either the `pivot_search` or `pivot_json` parameter.

Request parameters

Name	Type	Default	Description
pivot_json	String		JSON specifying a pivot based on the named data model. Typically, you URL encode this parameter. This endpoint requires either this pivot_json parameter or a pivot_search parameter.
pivot_search	String		A pivot search command based on the named data model. Typically, you URL encode this parameter. This endpoint requires either a pivot_json or this pivot_search parameter.

Returned values

Name	Description
drilldown_search	The search for running this pivot report using drilldown
open_in_search	Equivalent to search parameter, but listed more simply.
pivot_json	JSON specifying a pivot based on the named data model.
pivot_search	A pivot search command based on the named data model.
search	The search string for running the pivot report
tstats_search	The search for running this pivot report using tstats

Example request and response

XML Request

```
curl -k -u admin:pass -G https://localhost:8089/services/datamodel/pivot/Authentication --data-urlencode
pivot_search='| pivot Authentication Untagged_Authentication count(Untagged_Authentication) AS "Count of
Untagged Authentication (S.o.S)"'
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://localhost:8089/services/datamodel/pivot</id>
  <updated>2013-08-26T15:07:57-07:00</updated>
  <generator build="178683" version="20130826"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Authentication</title>
    <id>https://localhost:8089/servicesNS/nobody/search/datamodel/pivot/Authentication</id>
    <updated>2013-08-26T15:07:57-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/pivot/Authentication" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/pivot/Authentication" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="drilldown_search">| search (login OR "log in" OR authenticated) sourcetype!=stash NOT
tag=authentication | stats count AS "Count of Untagged Authentication (S.o.S)"  | fields , "Count of
Untagged Authentication (S.o.S)"| fillnull "Count of Untagged Authentication (S.o.S)"</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>is_pivot_command</s:item>
                <s:item>namespace</s:item>
                <s:item>pivot_json</s:item>
                <s:item>pivot_search</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:digest">e74d56a3b4a25256028f3a236e3d2cbc</s:key>
        <s:key name="eai:type">models</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="open_in_search">| search (login OR "log in" OR authenticated) sourcetype!=stash NOT
tag=authentication | stats count AS "Count of Untagged Authentication (S.o.S)"  | fields , "Count of
Untagged Authentication (S.o.S)"| fillnull "Count of Untagged Authentication (S.o.S)"</s:key>
        <s:key name="pivot_json"><![CDATA[{"rowFormat": {"showSummary": false}, "cells": [{"label": "Count
of Untagged Authentication (S.o.S)", "value": "count", "fieldName": "Untagged_Authentication", "type":
"objectCount", "owner": "Untagged_Authentication"}], "filters": [], "modelName": "Authentication",
"baseClass": "Untagged_Authentication", "rows": [], "columns": [], "colFormat": {"showSummary": false,
"showOther": true}}]]></s:key>
        <s:key name="pivot_search">| pivot Authentication Untagged_Authentication
count(Untagged_Authentication) AS "Count of Untagged Authentication (S.o.S)"</s:key>
        <s:key name="search">| search (login OR "log in" OR authenticated) sourcetype!=stash NOT
tag=authentication | stats count AS "Count of Untagged Authentication (S.o.S)"  | fields , "Count of
```

```
Untagged Authentication (S.o.S)"| fillnull "Count of Untagged Authentication (S.o.S)"</s:key>
        <s:key name="tstats_search"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

directory

`https://<host>:<mPort>/services/directory`

Access user configurable objects.

These objects includes search commands, UI views, UI navigation, saved searches and event types. This is useful to see which objects are provided by all apps, or a specific app when the call is namespaced.

GET

List app-scoped objects.

Usage details

Returns an enumeration of the following app scoped objects.

```
* event types
* saved searches
* time configurations
* views
* navs
* manager XML
* quickstart XML
* search commands
* tags
* field extractions
* lookups
* workflow actions
* field aliases
* sourcetype renames
```

This is useful to see which apps provide which objects, or all the objects provided by a specific app. To change the visibility of an object type in this listing, use the `showInDirSvc` setting in `restmap.conf`.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/directory
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:s="http://dev.splunk.com/ns/rest"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>directory</title>
  <id>https://localhost:8089/services/directory</id>
  <updated>2011-05-16T19:03:40-0700</updated>
  <generator version="98144"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>_admin</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/ui/views/_admin</id>
    <updated>2011-05-16T19:03:40-0700</updated>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin" rel="list"/>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:type">views</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>abc</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/ui/views/abc</id>
    <updated>2011-05-16T19:03:40-0700</updated>
    <link href="/servicesNS/nobody/search/data/ui/views/abc" rel="alternate"/>
    <author>
      <name>ssorkin</name>
    </author>
    <link href="/servicesNS/nobody/search/data/ui/views/abc" rel="list"/>
    <link href="/servicesNS/nobody/search/data/ui/views/abc/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/ui/views/abc" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:type">views</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

directory/{name}

`https://<host>:<mPort>/services/directory/{name}`
Get information about the `{name}` directory entity.

Usage details

This is rarely used. Typically after using the directory service enumeration, a client follows the specific link for an object in an enumeration.

GET

Get information about a specific directory entity.

Request parameters

None

Returned values

Name	Description
eai:type	Entity type.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/directory/dashboard_live
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>directory</title>
  <id>https://localhost:8089/services/directory</id>
  <updated>2011-05-16T19:09:59-0700</updated>
  <generator version="98144"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>dashboard_live</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/ui/views/dashboard_live</id>
    <updated>2011-05-16T19:09:59-0700</updated>
    <link href="/servicesNS/nobody/search/data/ui/views/dashboard_live" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/ui/views/dashboard_live" rel="list"/>
    <link href="/servicesNS/nobody/search/data/ui/views/dashboard_live/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/ui/views/dashboard_live" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
            <s:dict>
                <s:key name="optionalFields">
                    <s:list/>
                </s:key>
                <s:key name="requiredFields">
                    <s:list/>
                </s:key>
                <s:key name="wildcardFields">
                    <s:list/>
                </s:key>
            </s:dict>
        </s:key>
        <s:key name="eai:type">views</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/bookmarks/monitoring_console

`https://<host>:<mPort>/services/saved/bookmarks/monitoring_console`

Add URLs that link to monitoring consoles of your other deployments. For example, if you're admin overseeing multiple separate Splunk deployments for different teams.

GET

List deployment bookmarks.

Request parameters

Optional request parameters:

Name	Type	Description
count	Number	Number of bookmark URLs to list.
offset	Number	Lists bookmark URLs, offset from the first bookmark.

Name	Type	Description
search	String	Items to search for, must be valid as SPL.
sort_dir	Enum	asc or desc; ascending or descending
sort_key	String	Key to sort on, must be existing key in the stanza

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/saved/bookmarks/monitoring_console
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bookmarks-mc</title>
  <id>https://qa-ubuntu-022:8089/services/saved/bookmarks/monitoring_console</id>
  <updated>2019-10-13T16:47:42-07:00</updated>
  <generator build="324da9f5a506" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
  <link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
  <link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment-2</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>deployment-3</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-3/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="url">https://deployment-3-host:8000/en-US/app/splunk_monitoring_console</s:key>
    </s:dict>
  </content>
 </entry>
</feed>
```

POST

Add deployment bookmark URLs.

Request parameters

Name	Type	Description
name	String	Name of the deployment bookmark.
url	string	Full URL to the monitoring console of a different Splunk deployment.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/saved/bookmarks/monitoring_console -d
name=deployment-2 -d url=https://deployment-2-host:8000/en-US/app/splunk_monitoring_console
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bookmarks-mc</title>
  <id>https://localhost:8089/services/saved/bookmarks/monitoring_console</id>
  <updated>2019-10-13T16:16:38-07:00</updated>
  <generator build="324da9f5a506" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
  <link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
  <link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment-2</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

DELETE

Remove deployment bookmark URLs.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/saved/bookmarks/monitoring_console/{name}
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>bookmarks-mc</title>
  <id>https://localhost:8089/services/saved/bookmarks/monitoring_console</id>
  <updated>2019-10-13T16:25:38-07:00</updated>
  <generator build="324da9f5a506" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
  <link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
  <link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>deployment-2</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2<
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="remove"/>
    <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/eventtypes

`https://<host>:<mPort>/services/saved/eventtypes`

Access or create an event type.

GET

Retrieve saved event types.

Example

Request parameters

Pagination and filtering parameters can be used with this method.

Response data keys

Name	Description
description	Description of this event type.
disabled	Indicates if the event type is disabled.
eai:appName	The Splunk app for which this event type applies. For example, the Splunk search app.
eai:userName	Splunk user name of the creator of this event type. For example, the Splunk admin user.
priority	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
search	Search terms for this event type.
tags	[Deprecated] Tags associated with this event type. Use the tags.conf.spec file to assign tags to groups of events with related field values.

Returned values

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:46:52-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>internal_search_terms</title>
    <id>https://localhost:8089/servicesNS/nobody/system/saved/eventtypes/internal_search_terms</id>
    <updated>2011-07-10T23:46:52-07:00</updated>
    <link href="/servicesNS/nobody/system/saved/eventtypes/internal_search_terms" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/saved/eventtypes/internal_search_terms" rel="list"/>
    <link href="/servicesNS/nobody/system/saved/eventtypes/internal_search_terms/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/saved/eventtypes/internal_search_terms" rel="edit"/>
    <link href="/servicesNS/nobody/system/saved/eventtypes/internal_search_terms/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="description"/>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="priority">1</s:key>
        <s:key name="search">
<![CDATA[( "After evaluating args" OR "Before evaluating args" OR "context dispatched for search=" OR
"SearchParser - PARSING" OR "got search" OR "_dispatchNewSearch - search" OR "search:* - q" OR (
decomposition fullsearch ) OR "PAAAAAARSER! - search" OR "view:* - DECOMPOSITION" OR
"Splunk.Module.SearchBar .setInputField" OR ( typeahead prefix ) OR "DEBUG HTTPServer - Deleting
request=GET" OR /en-US/api/search/typeahead )]]>        </s:key>
        <s:key name="tags">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create an event type.

Request parameters

Name	Type	Default	Description
name	String		The name for the event type.
search	String		Search terms for this event type.
description	String		Human-readable description of this event type.
disabled	Boolean	0	If True, disables the event type.
priority	Number	1	Specify an integer from 1 to 10 for the value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
tags	String		[Deprecated] Use `tags.conf.spec` file to assign tags to groups of events with related field values.

Returned values

Name	Description
description	Description of this event type.
disabled	Indicates if this event type is disabled.
eai:appName	The Splunk app for which this event type applies. For example, the Splunk search app.
eai:userName	Splunk user name of the creator of this event type. For example, the Splunk admin user.
priority	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
search	Search terms for this event type.
tags	[Deprecated] Tags associated with this event type.

Name	Description
	Use tags.conf.spec file to assign tags to groups of events with related field values.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes -d
name="client-errors" --data-urlencode search=search="http client error NOT (403 OR 404)"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:47:10-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>client-errors</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors</id>
    <updated>2011-07-10T23:47:10-07:00</updated>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="list"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description"/>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="priority">1</s:key>
        <s:key name="search">search</s:key>
        <s:key name="tags">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/eventtypes/{name}

```
https://<host>:<mPort>/services/saved/eventtypes/{name}
```

Manage the `{name}` event type.

DELETE

Delete an event type.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:48:29-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access the `{name}` event type.

Requets parameters

None

Returned values

Name	Description
description	Description of this event type.
disabled	Indicates if the event type is disabled.
eai:appName	The Splunk app for which this event type applies. For example, the Splunk search app.
eai:attributes	Field control information.
eai:userName	Splunk user name of the creator of this event type. For example, the Splunk admin user.
priority	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
search	Search terms for this event type.
tags	[Deprecated] Tags associated with this event type. Use the tags.conf.spec file to assign tags to groups of events with related field values.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:47:17-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>client-errors</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors</id>
    <updated>2011-07-10T23:47:17-07:00</updated>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="alternate"/>
    <author>
```

```
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="list"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description"/>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>description</s:item>
                <s:item>disabled</s:item>
                <s:item>priority</s:item>
                <s:item>tags</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>search</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="priority">1</s:key>
        <s:key name="search">search</s:key>
        <s:key name="tags">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update an event type.

Usage details

The search must be re-specified for this edit.

URI-encode the search string if it contains any of the following characters: =, &, ?, %

If the search string is not URI-encoded, these characters can be interpreted as part of the HTTP request.

Request parameters

Name	Type	Default	Description
search	String		Search terms for this event type.
description	String		Human-readable description of this event type.
disabled	Boolean	0	If True, disables the event type.
priority	Number	1	Specify an integer from 1 to 10 for the value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
tags	String		[Deprecated] Use `tags.conf.spec` file to assign tags to groups of events with related field values.

Returned values

Name	Description
description	Description of this event type.
disabled	Indicates if this event type is disabled.
eai:appName	The Splunk app for which this event type applies. For example, the Splunk search app.
eai:userName	Splunk user name of the creator of this event type. For example, the Splunk admin user.
priority	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
search	Search terms for this event type.
tags	[Deprecated] Tags associated with this event type. Use tags.conf.spec file to assign tags to groups of events with related field values.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors -d
description="HTTP Client Errors" --data-urlencode search=search="http client error NOT (403 OR 404)"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:48:22-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>client-errors</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors</id>
    <updated>2011-07-10T23:48:22-07:00</updated>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="list"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description">HTTP Client Errors</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="priority">1</s:key>
        <s:key name="search">search</s:key>
        <s:key name="tags">
          <s:list/>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/fields

`https://<host>:<mPort>/services/search/fields`
Access search field configurations.

Usage details
Field configuration is specified in `$SPLUNK_HOME/etc/system/default/fields.conf`, with overriden values in `$SPLUNK_HOME/etc/system/local/fields.conf`.

GET

Get a list of fields registered for field configuration.

Request parameters

None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Fields</title>
  <id>/servicesNS/admin/search/search/fields</id>
  <updated>2011-07-11T10:04:51-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>_indextime</title>
    <id>/servicesNS/admin/search/search/fields/_indextime</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/_indextime" rel="alternate"/>
  </entry>
  <entry>
    <title>_sourcetype</title>
    <id>/servicesNS/admin/search/search/fields/_sourcetype</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/_sourcetype" rel="alternate"/>
  </entry>
  <entry>
    <title>date_hour</title>
    <id>/servicesNS/admin/search/search/fields/date_hour</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/date_hour" rel="alternate"/>
  </entry>

  . . . elided . . .

  <entry>
    <title>splunk_server</title>
    <id>/servicesNS/admin/search/search/fields/splunk_server</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/splunk_server" rel="alternate"/>
  </entry>
  <entry>
    <title>timeendpos</title>
    <id>/servicesNS/admin/search/search/fields/timeendpos</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/timeendpos" rel="alternate"/>
  </entry>
  <entry>
    <title>timestartpos</title>
    <id>/servicesNS/admin/search/search/fields/timestartpos</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/timestartpos" rel="alternate"/>
  </entry>
</feed>
```

search/fields/{field_name}

```
https://<host>:<mPort>/services/search/fields/{field_name}
```

Access the `{field_name}` field.

GET

Get information about the `{field_name}` field.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields/sourcetype
```

XML Response

```
<entry xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype</title>
  <id>/servicesNS/admin/search/search/fields/sourcetype</id>
  <updated>2011-07-11T10:08:54-07:00</updated>
  <link href="/servicesNS/admin/search/search/fields/sourcetype" rel="alternate"/>
  <content type="text">        Attr:INDEXED        True
        Attr:INDEXED_VALUE        False
        Attr:TOKENIZER
</content>
</entry>
```

search/fields/{field_name}/tags

```
https://<host>:<mPort>/services/search/fields/{field_name}/tags
```

Access or update the tags associated with the `{field_name}` field.

GET

Get tags associated with the `{field_name}` field.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields/host/tags
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Tags for the host field</title>
  <id>/servicesNS/admin/search/search/fields/host/tags</id>
  <updated>2011-07-11T10:41:46-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>location::sfo</title>
    <id>/servicesNS/admin/search/search/fields/host/tags#location::sfo</id>
    <updated>2011-07-11T10:41:46-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/host/tags#location::sfo" rel="alternate"/>
  </entry>
</feed>
```

POST

Update tags associated with the `{field_name}` field.

Usage details
The value parameter specifies the specific value on which to bind tag actions. Multiple tags can be attached by passing multiple add or delete form parameters. The server processes all of the adds first, and then processes the deletes.

You must specify at least one add or delete parameter.

Request parameters

Name	Type	Default	Description

value	String		The specific field value on which to bind the tags.
add	String		The tag to attach to this `field_name:value` combination.
delete	String		The tag to remove to this `field_name::value` combination.

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields/host/tags -d add=sfo -d
delete=nyc -d value=location
```

XML Response

```
<response>
  <messages>
    <msg type='INFO'>Successfully processed adds/deletes for field host</msg>
  </messages>
</response>
```

search/tags

`https://<host>:<mPort>/services/search/tags`
Access search time tags.

GET

List all search time tags.

Request parameters

None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/tags
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Tags</title>
  <id>/servicesNS/admin/search/search/tags</id>
  <updated>2011-07-08T01:35:09-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>machine</title>
    <id>/servicesNS/admin/search/search/tags/machine</id>
    <updated>2011-07-08T01:35:09-07:00</updated>
    <link href="/servicesNS/admin/search/search/tags/machine" rel="alternate"/>
  </entry>
  <entry>
    <title>user</title>
    <id>/servicesNS/admin/search/search/tags/user</id>
    <updated>2011-07-08T01:35:09-07:00</updated>
    <link href="/servicesNS/admin/search/search/tags/user" rel="alternate"/>
  </entry>
</feed>
```

search/tags/{tag_name}

`https://<host>:<mPort>/services/search/tags/{tag_name}`
Access, update, or delete `{tag_name}` values.

DELETE

Delete the tag and its associated field:value pair assignments.

Usage details

When a tag is deleted, field:value pairs are set to `disabled` in `tags.conf`.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/servicesNS/admin/search/search/tags/user
```

XML Response

```
<response>
  <messages>
    <msg type="INFO">Tag successfully deleted</msg>
  </messages>
</response>
```

GET

Returns a list of field:value pairs associated with the `{tag_name}` tag.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/tags/user
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Field::Value pairs with tag user</title>
  <id>/servicesNS/admin/search/search/tags/user</id>
  <updated>2011-07-08T01:35:28-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>eventtype::userupdate</title>
    <id>/servicesNS/admin/search/search/tags/user#eventtype::userupdate</id>
    <updated>2011-07-08T01:35:28-07:00</updated>
    <link href="/servicesNS/admin/search/search/tags/user#eventtype::userupdate" rel="alternate"/>
  </entry>
</feed>
```

POST

Update the field:value pairs associated with the {tag_name} tag.

Usage details

Multiple field:value pairs can be attached by passing multiple add or delete form parameters. The server processes all of the adds first, and then deletes.

If `{tag_name}` does not exist, then the tag is created inline. Notification is sent to the client using the HTTP 201 status.

Request parameters

Name	Type	Default	Description
add	String		A field:value pair to tag with {tag_name}.
delete	String		A field:value pair to remove from {tag_name}.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/tags/user -d
add=eventtype::userupdate -d delete=eventtype::useradd-suse
```

XML Response

```
<response>
  <messages>
    <msg type="INFO">Processed adds/deletes for tag</msg>
  </messages>
</response>
```

KV store endpoints

KV store endpoint descriptions

This introduction describes syntax common to all app KV Store REST endpoints. For more information about the KV Store, see App Key Value Store on the Splunk developer portal.

REST API usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API.

Some but not all KV store endpoints are available in Splunk Cloud Platform. Instead, authorized users can access and configure the KV store lookup definitions in the Splunk Cloud Platform user interface. KV store collections, however, cannot be modified with the user interface.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

App KV Store REST API features

The app KV Store provides the following functions.

- Create, read, list and delete EAI operations on a collection.
- Create, read, list and delete indexes for a given collection. All collection methods are EAI-compatible. These are not regular EAI operations because the indexes are stored as attributes on the EAI entity. Users must have collection permission to use these operations for a particular collection.
- The ability to insert, read, update and delete a single key and key value, for a given collection, provided that you have permission to modify the collection.

    - Duplicate keys are not allowed.
    - All updates are wholesale updates.
    - Partial value updates are not available.
- The ability to query key-value pairs, for a given collection. For example, to find all the documents that have a host field with a value, use the query `{"host": "bar.com"}`.

Only the following operations are permitted.

- `$gt`
- `$gte`
- `$lt`
- `$lte`
- `$ne`
- `$and`
- `$or`,
- `$not`.

The API also supports mechanisms for projection, sorting and pagination.

- Batch reads, inserts, and/or updates for a given collection. This supports high-volume operations and limits network traffic. These operations have the same semantics as their individual counterparts.

Limits

- 16MB per record
- 1KB per accelerated field

Collections

A Collection is a container of "documents" or "values". Most documents have a similar structure, although structure is not enforced. For example, a Collection might have `Notable Events` or `entities`.

Collections are declared in a `collections.conf` configuration file, where a stanza is a single collection.

Collection permissioning

Collections are Splunk entities, which means they are permissioned using the Splunk RBAC/ACL system. Only app-level permissions are available for collections. This means that collections can be defined only in the `etc/apps/<app>/<default|local>` directory, not in `etc/users/...`. Attempts to create a user-specific Collection using the API fail and Collections created manually in the `.conf` files are ignored.

Data

A collection stores key-value pairs consisting of a user-specified or autogenerated key and a JSON document-formatted value. A JSON document/object of values is enforced for simplicity instead of using integer or string raw values. For example, `{"_key": "10.0.0.1", host: "bar.com"}` defines the key (`"10.0.0.1"`) and the full JSON document value.

A key is fetched, updated, and deleted. Partial updates, including array append, are not available. You must set the whole document. Keys are unique within a collection and support only the basic JSON data types: boolean, string, number, object, array, and `null`.

A value is specified in the `_key` attribute of the document and, if one is not specified, a random value with a desirable sort order is automatically generated.

A collection is defined in the following directory location.

```
/servicesNS/nobody/search/storage/collections/mycollection
```

You can use the following URLs to access the collection.

- /servicesNS/nobody/search/storage/collections/mycollection
- /servicesNS/itay/search/storage/collections/mycollection
- /servicesNS/mark/search/storage/collections/mycollection

Namespaces are separate and data are not interleaved. Wildcard operations on the `<user>` or `<app>` parts of the namespace are not available.

User-specific collections are not supported. All users, including `nobody`, share a single namespace and `_key` is unique across all namespaces.

Types

You can define a set of types for some fields in a collection. If a field has no type defined, it uses the type submitted over the API. If a type conversion fails, the insert/update operation is aborted.

Here is an example collection in `collections.conf`.

```
[mycollection]
field.enabled = bool
field.data.range = cidr
```

The data inserted or updated in this collection have the fields enabled and range-converted to the applicable type.

```
* array
* number
* boolean
* time
* string
* cidr
```

Items need to be specified using the `field` prefix only if type needs to be enforced for the field. The `array` type is not enforceable so does not need to be specified.

Arrays

Arrays do not change a nested key name. For example, the key "a.b.c" can refer to `{"a": {"b": {"c": 1}}}` or `{"a": {"b": [{"c": 1}]}}`.

Numbers

All strings/numbers/booleans are converted to doubles. If a number fails to convert, it inserts the string instead.

Booleans

All numbers/strings/booleans are converted to booleans. If a boolean fails to convert, it inserts the string instead. Epoch time can be a string or a number. If it fails to convert, the string version is inserted.

Strings

Everything is converted to a string.

CIDR

All provided strings are converted to canonical CIDR strings. Here is an example.

```
127.0.0.1        -> 127.000.000.001/32
127.0.0.0/24     -> 127.000.000.000/24
127.0.0/24       -> 127.000.000.000/24
```

Here is an example of similar canonicalization for IPv6.

```
2001:db8::/96               -> 2001:0db8:0000:0000:0000:0000:0000:0000/096
2001:db8:0:0:0:0:0:ffff     -> 2001:0db8:0000:0000:0000:0000:0000:ffff/128
```

Queries

Combining the Data and Index patterns gives the ability to do basic querying. Queries are limited to the basic operators available in most databases, and at the moment do not expose in-array and not-in-array containers. A query can have the following operators.

- gt
- gte
- lt
- lte
- eq
- neq
- or
- and
- not

Queries are permitted regardless of whether an index covers the query. If it the index does not cover the query, the query takes longer to complete. For example, here is a query to find all `Notable Events` authored by userA or userB.

```
{ "$or": [ { "author": "userA" }, { "author": "userB" } ] }
```

Use `$and` to search for a range of values. For example, use the following query to find all events with a time field value between `12` and `13`.

```
{ "$and": [ { "time": { "$gt": "12" } }, { "time": { "$lt": "13" } } ] }
```

REST methods

The REST API for App KV Store implements the GET, POST, and DELETE methods described in this reference.

Defining KV Store lookups

For information on using the REST API to define or update a KV Store lookup, see `data/transforms/lookups/` and `data/transforms/lookups/{name}`.

kvstore/backup/create

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/kvstore/backup/create
```
POST

Create a KV Store backup archive file.

Usage details

Request parameters

Name	Type	Description
archiveName	String	Specify a file name for the backup.
appName	String	Specify a target app for backup, rather than all of the KV Store. Only available if *pointInTime* is not set to true.
collectionName	String	Specify a target collection for backup, rather than all of the KV Store. Only available if *pointInTime* is not set to true.
pointInTime	Boolean	Defaults to false. To take a consistent backup, set it to true. Only available for single-instance deployments.
cancel	Boolean	Defaults to false. Set it to true to cancel an in-progress backup. Only available if *pointInTime* is set to true.
parallelCollections	Number	Defaults to 1. Raise the number to increase the number of collections to back up in parallel. Only available if *pointInTime* is set to true.

Returned values

Name	Description
status	Code `200` for success, and code `404` for failure.

Example request and response

XML request

```
curl -k -u admin:changed -X POST https://localhost:8089/services/kvstore/backup/create -d
'archiveName=sampleArchive&appName=search&collectionName=testcollection'
```

XML response

```
  <title>kvstorebackup</title>
  <id>https://localhost:8089/services/kvstore/backup</id>
  <updated>2018-04-05T14:18:14-07:00</updated>
  <generator build="dbd2996dbabd8f6751329c845684e0ffc9d1cca3" version="20180302"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/kvstore/backup/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

kvstore/backup/restore

This endpoint is available in Splunk Enterprise only.

`https://<host>:<mPort>/services/kvstore/backup/restore`
POST

Extracts the KV Store backup archive file and restores the KV Store.

Usage details

Request parameters

Name	Type	Description
archiveName	String	**Required**. Specifies the name of the backup file.
appName	String	Specify a target app for backup, rather than all of the KV Store. Only available if *pointInTime* is not set to true.
collectionName	String	Specify a target collection for backup, rather than all of the KV Store. Only available if *pointInTime* is not set to true.
pointInTime	Boolean	Defaults to false. To restore from a backup taken with consistency, set it to true.
cancel	Boolean	Defaults to false. Set it to true to cancel an in-progress restore. Only available if *pointInTime* set to true.
parallelCollections	Number	Defaults to 1. Raise the number to increase the number of collections to restore in parallel, which speeds up the store. Only available if *pointInTime* set to true.
insertionsWorkersPerCollection	Number	Defaults to 1. Raise to increase the number of insertion workers per collection, which speeds up the restore. Only available if *pointInTime* set to true.

Returned values

Name	Description
status	Code `200` for success, and code `404` for failure.

Example request and response

XML request

```
curl -k -u admin:changed -X POST https://localhost:8089/services/kvstore/backup/restore -d
'archiveName=kvdump.tar.gz&appName=search&collectionName=testcollection'
```

XML response

```
  <title>kvstorebackup</title>
  <id>https://localhost:8089/services/kvstore/backup</id>
  <updated>2018-04-05T14:10:00-07:00</updated>
  <generator build="dbd2996dbabd8f6751329c845684e0ffc9d1cca3" version="20180302"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/kvstore/backup/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

kvstore/control/maintenance

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/kvstore/control/maintenance
```

Access KV store maintenance mode for standalone deployments.

POST

Toggle maintenance mode.

Request parameters

Name	Type	Description
mode	Boolean	**Required.** Type *true* to enter maintenance mode. To exit, type *false*.

Example request and response

XML Request

```
curl -ku admin:changeme -X POST https://localhost:8089/services/kvstore/control/maintenance -d 'mode=false'
```

XML Response

```
<title>kvstorecontrol</title>
  <id>https://localhost:8089/services/kvstore/control</id>
  <updated>2021-03-29T14:53:25-07:00</updated>
  <generator build="c470713bc601c2961f6dba368c5b4c6628687211" version="20210304"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/kvstore/control/maintenance" rel="maintenance"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

kvstore/status

`https://<host>:<mPort>/services/kvstore/status`
Access KV store status information for standalone or search head clustering (SHC) deployments. For SHC deployments, provides information on SHC members where KV Store is enabled and used for replication.

See also the following KV Store introspection endpoints.

- server/introspection/kvstore
- server/introspection/kvstore/collectionstats
- server/introspection/kvstore/replicasetstats
- server/introspection/kvstore/serverstatus

GET

Access KV store status information.

Usage details

Request parameters

None.

Returned values

Name	Description
current	Includes the following indicators for the machine making the GET request. • `backupRestoreStatus`: Status for a KV Store backup in progress. One of the following values: ♦ `Busy`: Backup or restore in progress. ♦ `Failed`: Restore failed to extract an archive file. ♦ `Ready`: Ready to run a backup or restore. ♦ `Shutdown`: KV Store is in the process of shutting down. • `backupRestoreProgress`: Counter that increments each time a collection finishes being backed up or restored. • `date`: DateTime when this status was retrieved. • `datesec`: Unix timestamp, equivalent to `date` • `disabled`: If KV Store is disabled on the current member. `0` means enabled, `1` means disabled. • `guid`: Instance ID of the current member. • `oplogEndTimestamp`: Last recorded timestamp in the operations log. Last update in all KV Store collections. Compare this indicator to other instances to check if KV Store members are not up to date. • `oplogEndTimestampSec`: Unix timestamp equivalent to `oplogEndTimestamp` • `oplogStartTimestamp`: First recorded timestamp in the operations log. • `oplogStartTimestampSec`: Unix timestamp equivalent to `oplogStartTimestamp` • `port`: KV Store port

Name	Description
	• replicaSet: Replica set name. Instance ID by default for standalone mode. Configured in server.conf for SHC. • replicationStatus: In standalone mode, this is KV Store captain. Otherwise, one of the following values. ♦ Startup ♦ KV Store captain ♦ Non-captain KV Store member ♦ Recovering ♦ Initial Sync ♦ Unknown status ♦ Down ♦ Rollback ♦ Removed • standalone: Indicates whether the machine making the request is a standalone member or SHC member. 1 indicates a standalone member. • status: KV Store status. One of the following values. ♦ unknown ♦ disabled ♦ starting ♦ ready ♦ failed ♦ shuttingdown
Enabled KV Store members	Returned for SHC deployments. Lists the following values for SHC members where KV Store is enabled and used for replication. • guid: Instance ID of the current member. • hostAndPort: Address used for replication between KV Store members and for accessing members from splunkd. Can be configured in server.conf.
members	For KV Store members, lists the following indicators. • configVersion: Version number that increases each time the KV Store cluster is updated. • electionDate: DateTime for election. • electionDateSec: Unix equivalent of electionDate • hostAndPort: Address used for replication between KV Store members and for accessing members from splunkd. Can be configured in server.conf. • lastHeartbeat: Last time the requesting member sent a heartbeat to this member. • lastHeartbeatRecv: Last time this member replied on heartbeat. • lastHeartbeatRecvSec: Unix equivalent of lastHeartbeatRecv • lastHeartbeatSec: Unix equivalent of lastHeartbeat • optimeDate: Last recorded timestamp for this member in the operations log. • optimeDateSec: Unix equivalent of optimeDate • pingMs: Latency (milliseconds for round trip. • replicationStatus: In standalone mode, this is KV Store captain. Otherwise, one of the following values. ♦ Startup ♦ KV Store captain ♦ Non-captain KV Store member ♦ Recovering ♦ Initial Sync ♦ Unknown status ♦ Down ♦ Rollback ♦ Removed • uptime: Number of seconds this member has been online.

Example request and response

XML request

```
curl -k -u admin:changed https://localhost:8089/services/kvstore/status
```

XML response

```
  <title>kvstorestatus</title>
  <id>https://localhost:8089/services/kvstore/status</id>
  <updated>2016-09-09T15:04:35-07:00</updated>
  <generator build="c9afb322d148" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/kvstore/status/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>status</title>
    <id>https://localhost:8089/services/kvstore/status/status</id>
    <updated>2016-09-09T15:04:35-07:00</updated>
    <link href="/services/kvstore/status/status" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/kvstore/status/status" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="current">
          <s:dict>
            <s:key name="backupRestoreStatus">Ready</s:key>
            <s:key name="date">Fri Sep  9 15:04:35 2016</s:key>
            <s:key name="dateSec">1473458675.554000</s:key>
            <s:key name="disabled">0</s:key>
            <s:key name="guid">B4E173F1-02AA-4D46-9DDC-ECF0016F165E</s:key>
            <s:key name="oplogEndTimestamp">Fri Sep  9 14:17:01 2016</s:key>
            <s:key name="oplogEndTimestampSec">1473455821.000000</s:key>
            <s:key name="oplogStartTimestamp">Fri Sep  9 07:16:53 2016</s:key>
            <s:key name="oplogStartTimestampSec">1473430613.000000</s:key>
            <s:key name="port">8191</s:key>
            <s:key name="replicaSet">B4E173F1-02AA-4D46-9DDC-ECF0016F165E</s:key>
            <s:key name="replicationStatus">KV store captain</s:key>
            <s:key name="standalone">1</s:key>
            <s:key name="status">ready</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
```

```
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="members">
          <s:dict>
            <s:key name="0">
              <s:dict>
                <s:key name="configVersion">1</s:key>
                <s:key name="electionDate">Fri Sep  9 07:16:53 2016</s:key>
                <s:key name="electionDateSec">1473430613.000000</s:key>
                <s:key name="hostAndPort">127.0.0.1:8191</s:key>
                <s:key name="lastHeartbeat"></s:key>
                <s:key name="lastHeartbeatRecv"></s:key>
                <s:key name="lastHeartbeatRecvSec"></s:key>
                <s:key name="lastHeartbeatSec"></s:key>
                <s:key name="optimeDate">Fri Sep  9 14:17:01 2016</s:key>
                <s:key name="optimeDateSec">1473455821.000000</s:key>
                <s:key name="pingMs"></s:key>
                <s:key name="replicationStatus">KV store captain</s:key>
                <s:key name="uptime">28071</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

services/kvstore/version

This endpoint is available in Splunk Enterprise only.

`https://localhost:8099/services/kvstore/version`
Check the status of a KV store server version upgrade in a single-instance deployment.

GET

Check the status.

Request parameters

None.

Returned values

Name	Description

migrationID	ID number for the upgrade.
migrationStartTime	Timestamp that the upgrade began.
peerRetryCount	Number of times that the upgrade failed and retried.
status	Status of the upgrade.
version	Target version.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8099/services/kvstore/version
```

XML Response

```
...
        <content type="text/xml">
            <s:dict>
                <s:key name="eai:acl">
                    <s:dict>
                        <s:key name="app"></s:key>
                        <s:key name="can_list">1</s:key>
                        <s:key name="can_write">1</s:key>
                        <s:key name="modifiable">0</s:key>
                        <s:key name="owner">system</s:key>
                        <s:key name="perms">
                            <s:dict>
                                <s:key name="read">
                                    <s:list>
                                        <s:item>admin</s:item>
                                        <s:item>splunk-system-role< /s:item>
                                        <s:item>splunk_system_upgrader< /s:item>
                                    </s:list>
                                </s:key>
                                <s:key name="write">
                                    <s:list>
                                        <s:item>admin</s:item>
                                        <s:item>splunk-system-role< /s:item>
                                    </s:list>
                                </s:key>
                            </s:dict>
                        </s:key>
                        <s:key name="removable">0</s:key>
                        <s:key name="sharing">system</s:key>
                    </s:dict>
                </s:key>
                <s:key name="status">
                    <s:dict>
                        <s:key name="storageEngine">wiredTiger</s:key>
                        <s:key name="upgradeStatus">1</s:key>
                        <s:key name="version">4.2.25</s:key>
                    </s:dict>
                </s:key>
            </s:dict>
        </content>
```

services/kvstore/version/stop_upgrade

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/kvstore/version/stop_upgrade
```

Stop upgrade of the KV store server version on a single-instance deployment.

POST

Stop the upgrade.

Request parameters

None.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8099/services/kvstore/version/stop_upgrade
```

XML Response

```
...
    <author>
        <name>Splunk</name>
    </author>
    <link href="/services/kvstore/version/stop_upgrade" rel="stop_upgrade"/>
    <link href="/services/kvstore/version/upgrade" rel="upgrade"/>
    <opensearch:totalResults>0</opensearch:totalResults>
    <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
    <opensearch:startIndex>0</opensearch:startIndex>
    <s:messages/>
```

services/kvstore/version/upgrade

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/kvstore/version/upgrade
```

Start upgrade of the KV store server version on a single-instance deployment.

POST

Start the upgrade.

Request parameters

Name	Type	Description
version	Number	**Required.** Target version number to upgrade to, such as `7.0`.
isDryRun	Boolean	Set to `'true` to complete pre-flight checks and exit without upgrading. Setting is `false` by default.
maxRetries	Number	Number of times to retry a failed upgrade.

Example request and response

XML Request

```
curl -ku admin:changeme -X POST https://localhost:8089/services/kvstore/version/upgrade -d version=7.0 -d
dryRun=true
```

XML Response

```
        <content type="text/xml">
            <s:dict>
                <s:key name="eai:acl">
                    <s:dict>
                        <s:key name="app"></s:key>
                        <s:key name="can_list">1</s:key>
                        <s:key name="can_write">1</s:key>
                        <s:key name="modifiable">0</s:key>
                        <s:key name="owner">system</s:key>
                        <s:key name="perms">
                            <s:dict>
                                <s:key name="read">
                                    <s:list>
                                        <s:item>admin</s:item>
                                        <s:item>splunk-system-role< /s:item>
                                        <s:item>splunk_system_upgrader< /s:item>
                                    </s:list>
                                </s:key>
                                <s:key name="write">
                                    <s:list>
                                        <s:item>admin</s:item>
                                        <s:item>splunk-system-role< /s:item>
                                    </s:list>
                                </s:key>
                            </s:dict>
                        </s:key>
                        <s:key name="removable">0</s:key>
                        <s:key name="sharing">system</s:key>
                    </s:dict>
                </s:key>
                <s:key name="upgrade">
                    <s:dict>
                        <s:key name="version">7.0</s:key>
                    </s:dict>
                </s:key>
            </s:dict>
        </content>
```

shcluster/captain/kvstore-upgrade/start

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/shcluster/captain/kvstore-upgrade/start
```

Start upgrade of the KV store server version in a clustered deployment.

POST

Start the upgrade.

Request parameters

Name	Type	Description
version	Number	**Required.** Target version number to upgrade to, such as `7.0`.
isDryRun	Boolean	Set to `true` to complete pre-flight checks and exit without upgrading. Setting is `false` by default.

Example request and response

XML Request

```
curl -k -u admin:changeme -X POST
https://localhost:8089/services/shcluster/captain/kvstore-upgrade/start?version=7.0
```

XML Response

```
...
  <s:messages>
    <s:msg type="INFO">SHC KV Store upgrade has been successfully triggered</s:msg>
  </s:messages>
```

shcluster/captain/kvstore-upgrade/status

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/shcluster/captain/kvstore-upgrade/status
```

See the status of KV store server version upgrade in a clustered deployment.

GET

See KV store server version upgrade status.

Request parameters

None.

Returned values

Name	Description
clusterPerc	Percentage of cluster members that have completed migration.
peerRetryCount	Number of times that the peer failed to update and retried.
result	Result of a completed upgrade.
startTime	Time the upgrade began.
status	Status of the overall upgrade.
updateID	ID number for the update.
version	Target version.
attempt_number	Number of attempted upgrades, not including the one in progress. Provided for each peer.
updateStatus	Status of the upgrade. Provided for each peer.

Example request and response

XML Request

```
curl -k -u admin:changeme -X GET https://localhost:8089/services/shcluster/captain/kvstore-upgrade/status
```

XML Response

```
 <title>kvstore-upgrade-status</title>
    <id>https://sh3:8089/services/shcluster/captain/kvstore-upgrade/kvstore-upgrade-status</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/shcluster/captain/kvstore-upgrade/kvstore-upgrade-status" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/kvstore-upgrade/kvstore-upgrade-status" rel="list"/>
    <link href="/services/shcluster/captain/kvstore-upgrade/kvstore-upgrade-status" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
```

```
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                    <s:item>splunk_system_upgrader</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      <s:key name="general">
          <s:dict>
            <s:key name="clusterPerc">100</s:key>
            <s:key name="peerRetryCount">1</s:key>
            <s:key name="result"></s:key>
            <s:key name="startTime">Thu Nov 14 00:50:32 2024</s:key>
            <s:key name="status">kvstore_upgrade_started</s:key>
            <s:key name="updateID">1731545432</s:key>
            <s:key name="version">7.0</s:key>
          </s:dict>
        </s:key>
        <s:key name="peerStatus">
          <s:dict>
            <s:key name="https://sh1:8089">
              <s:dict>
                <s:key name="attempt_number">0</s:key>
                <s:key name="updateStatus">aborted</s:key>
              </s:dict>
            </s:key>
            <s:key name="https://sh2:8089">
              <s:dict>
                <s:key name="attempt_number">0</s:key>
                <s:key name="updateStatus">in_progress</s:key>
              </s:dict>
            </s:key>
            <s:key name="https://sh3:8089">
              <s:dict>
                <s:key name="attempt_number">0</s:key>
                <s:key name="updateStatus">in_progress</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

shcluster/captain/kvstore-upgrade/stop

This endpoint is available in Splunk Enterprise only.

```
https://<host>:<mPort>/services/shcluster/captain/kvstore-upgrade/stop
```

Stop the KV store server version upgrade in a clustered deployment.

POST

Stop KV store server version upgrade.

Request parameters

None.

Example request and response

XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/shcluster/captain/kvstore-upgrade/stop
```

XML Response

```
   <s:messages>
    <s:msg type="INFO">KV Store upgrade stop initiated</s:msg>
  </s:messages>
```

shcluster/captain/kvmigrate/start

This endpoint is deprecated and removed in Splunk Enterprise 9.4 and higher.

```
https://<host>:<mPort>/services/shcluster/captain/kvmigrate/start
```

Start migration of the KV store storage engine.

POST

Start the migration.

Request parameters

Name	Type	Description

storageEngine	String	**Required.** Name of target storage engine, *wiredTiger* or *mmap*.
isDryRun	Boolean	Type *true* to complete pre-flight checks and exit without migrating. Setting is *false* by default.
maxRetries	Number	Number of times to retry a failed migration, per member.
clusterPerc	Number	Percentage of peers to migrate.
peersList	String	Names of peers to migrate, listed with name and management port. For example: `peersList="server1:8089,server2:8089,server3:8089"`

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8099/services/shcluster/captain/kvmigrate/start -X POST -d
storageEngine=wiredTiger -d clusterPerc=50
```

XML Response

```
.  <s:messages>

    <s:msg type="INFO">SHC KV Store migration has been successfully triggered</s:msg>

  </s:messages>
```

shcluster/captain/kvmigrate/status

This endpoint is deprecated and removed in Splunk Enterprise 9.4 and higher.

```
https://localhost:8099/services/shcluster/captain/kvmigrate/status
```

Check the status of a KV store storage engine migration.

GET

Check the status.

Request parameters

None.

Returned values

Name	Description
clusterPerc	Percentage of cluster members that have completed migration.
migrationID	ID number for the migration.
migrationStartTime	Timestamp that the migration began.

Name	Description
peerRetryCount	Number of times that the peer failed to migrate and retried.
status	Status of the migration.
storageEngine	Target storage engine.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8099/services/shcluster/captain/kvmigrate/status
```

XML Response

```
...
        <s:key name="general">
          <s:dict>
            <s:key name="clusterPerc">50</s:key>
            <s:key name="migrationID">1596760435</s:key>
            <s:key name="migrationStartTime">Thu Aug  6 17:33:55 2020</s:key>
            <s:key name="peerRetryCount">1</s:key>
            <s:key name="status">kvstore_migration_started</s:key>
            <s:key name="storageEngine">wiredTiger</s:key>
          </s:dict>
        </s:key>
        <s:key name="peerStatus">
          <s:dict>
            <s:key name="https://fool02:8099">
              <s:dict>
                <s:key name="attempt_number">1</s:key>
                <s:key name="migrationStatus">migration_in_progress</s:key>
              </s:dict>
            </s:key>
            <s:key name="https://fool02:8103">
              <s:dict>
                <s:key name="attempt_number">1</s:key>
                <s:key name="migrationStatus">migration_succeeded</s:key>
              </s:dict>
            </s:key>
```

shcluster/captain/kvmigrate/stop

> This endpoint is deprecated and removed in Splunk Enterprise 9.4 and higher.

```
https://<host>:<mPort>/services/shcluster/captain/kvmigrate/stop
```

Stop the migration of your KV store storage engine.

POST

Stop the migration.

Request parameters
None.

Example request and response

XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8099/services/shcluster/captain/kvmigrate/stop
```

XML Response

```
...
  <s:messages>

    <s:msg type="INFO">KV Store migration stop initiated</s:msg>

  </s:messages>
```

storage/collections/config

```
https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/config
```

Access and create collections.

GET

List all collections.

Request parameters
None.

Returned values

Name	Description
disabled	Boolean indicating collection state. By default, the value is `false`, indicating that the collection is enabled.
profilingEnabled	Boolean indicating profiling status of slow-running operations. By default, this value is `false`, meaning that profiling is disabled.
profilingThresholdMs	Threshold for logging slow-running operations, in milliseconds. Applies only if *profilingEnabled* is `true`.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config
```

XML Response

```
...
<title>collections-conf</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-09-02T11:28:27-07:00</updated> <generator build="229629" version="6.2"/>

<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/>
<link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>kvstoredemo</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/kvstoredemo</id>
  <updated>2014-09-02T11:28:27-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo" rel="remove"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl"> ... elided ... </s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="profilingEnabled">false</s:key>
      <s:key name="profilingThresholdMs">100</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>test</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test</id>
  <updated>2014-09-02T11:28:27-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="remove"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl"> ... elided ...</s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="profilingEnabled">false</s:key>
      <s:key name="profilingThresholdMs">100</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Create a collection.

Request parameters

Name	Type	Description
name	String	**Required**. Collection name
profilingEnabled	Boolean	A `collections.conf` file property that affects *profilingThresholdMs*. Defaults to `false`. Enable profiling of slow-running operations by setting *profilingEnabled* to `true`.
profilingThresholdMs	Number	Threshold for logging slow-running operations, in milliseconds. Applies only if *profilingEnabled* is `true`. Defaults to `100`. Set to `0` to log all slow-running operations.

Returned values

Name	Description
disabled	Boolean indicating collection state. By default, the value is `false`, indicating that the collection is enabled.
profilingEnabled	Profiling status of slow-running operations, *profilingThresholdMs*. Defaults to `false`.
profilingThresholdMs	Threshold for logging slow-running operations, in milliseconds. Applies only if *profilingEnabled* is `true`.

Example request and response

XML Request

```
curl -k -u admin:changeme -d name=test1
https://localhost:8089/servicesNS/nobody/search/storage/collections/config
```

XML Response

```
...
<title>collections-conf</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-09-02T11:25:32-07:00</updated> <generator build="229629" version="6.2"/>

<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/>
<link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
```

```
  <title>test1</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test1</id>
  <updated>2014-09-02T11:25:32-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/collections/config/test1" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/collections/config/test1" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test1/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test1" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test1" rel="remove"/>
  <link href="/servicesNS/nobody/search/storage/collections/config/test1/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl"> ... elided ... </s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="profilingEnabled">false</s:key>
      <s:key name="profilingThresholdMs">100</s:key>
    </s:dict>
  </content>
</entry>
```

storage/collections/config/{collection}

`https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/config/{collection}`

Access, delete, or update a specific `{collection}`.

DELETE

Delete a specific `{collection}`.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test -X
DELETE
```

XML Response

```
...
 <title>collections-conf</title>
```

```
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-06-02T20:08:11-07:00</updated>
<generator build="210538" version="20140530"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/>
<link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
```

GET

Access a specific `{collection}`.

Request parameters

None

Returned values

Name	Description
disabled	Boolean indicating collection state. By default, the value is `0`, meaning that the collection is enabled.
field.<fieldName>	Field type. One of the following values. - `array` - `number` - `bool` - `string` - `cidr` - `time`
accelerated_fields.<field_name>	Field acceleration name and JSON definition.
enforceTypes	Boolean indicating if data types are enforced when inserting data into the collection. Defaults to `false`.
profilingEnabled	Profiling status of slow-running operations, affecting *profilingThresholdMs*. By default, the value is `false`, meaning that profiling is disabled. If `true`, profiling is enabled.
profilingThresholdMs	Threshold for logging slow-running operations, in milliseconds. Applies only if *profilingEnabled* is `true`.
replicate	Boolean indicating whether the collection is replicated on indexers. Defaults to `false`, meaning that this collection is not replicated, and lookups that depend on the collection will not be available. However, if you run a lookup command with `local=true`, local lookups will still be available. When `true`, this collection is replicated on indexers.
replication_dump_maximum_file_size	Indicates the maximum file size (in KB) for each dump file when *replication_dump_strategy*=`auto`. Defaults to 10240KB. If this value is larger than `concerningReplicatedFileSize`, which is set in the `distsearch.conf` file, the value of `concerningReplicatedFileSize` is used instead. KV Store does not pre-calculate the size of the records that will be written to disk, so the size of the resulting files can be affected by the `max_rows_in_memory_per_dump` setting in the `limits.conf` file.

Name	Description
replication_dump_strategy	One of the following two values. • `auto`: Default. Dumps are stored in multiple files when the size of the collection exceeds the value of *replication_dump_maximum_file_size*. • `one_file`: Dump files are stored in a single file.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test
```

XML Response

```
...
<title>collections-conf</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-09-02T11:42:54-07:00</updated> <generator build="229629" version="6.2"/>

<author>

 <name>Splunk</name>
</author> <link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/> <link
href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/> ... opensearch nodes
elided ... <s:messages/> <entry>

 <title>test</title>
 <id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test</id>
 <updated>2014-09-02T11:42:54-07:00</updated>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="alternate"/>
 <author>
   <name>admin</name>
 </author>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="list"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test/_reload" rel="_reload"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="edit"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="remove"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test/disable" rel="disable"/>
 <content type="text/xml">
   <s:dict>
     <s:key name="disabled">0</s:key>
     <s:key name="eai:acl"> ... elided ... </s:key>
     <s:key name="eai:appName">search</s:key>
     <s:key name="eai:attributes"> ... elided ... </s:key>
     <s:key name="eai:userName">nobody</s:key>
     <s:key name="profilingEnabled">false</s:key>
     <s:key name="profilingThresholdMs">100</s:key>
   </s:dict>
 </content>
</entry>
```

POST

Update a specific `{collection}`.

Request parameters

Name	Type	Description
field.<fieldName>	String	Field type. One of the following values. • `array` • `number` • `bool` • `string` • `cidr` • `time`
accelerated_fields.<field_name>	String, JSON (see description)	The name of a field acceleration (string) and its definition, in JSON key value format. For example, `accelerated_fields.my_accel = {"id": 1}`

Returned values

Name	Description
disabled	Collection state: `true` = disabled. `false` = [Default] enabled.
field.<fieldName>	Field type. One of the following values. • `array` • `number` • `bool` • `string` • `cidr` • `time`
accelerated_fields.<field_name>	The name of a field acceleration (string) and its definition, in JSON key value format. For example, `accelerated_fields.my_accel = {"id": 1}`
profilingEnabled	Profiling status of slow-running operations, affecting *profilingThresholdMs*. By default, the value is `false`, meaning that profiling is disabled. If `true`, profiling is enabled.
profilingThresholdMs	Threshold for logging slow-running operations, in milliseconds. Applies only if *profilingEnabled* is `true`.
replicate	Boolean indicating whether the collection is replicated on indexers. Defaults to `false`, meaning that this collection is not replicated, and lookups that depend on the collection will not be available. However, if you run a lookup command with `local=true`, local lookups will still be available. When `true`, this collection is replicated on indexers.
replication_dump_maximum_file_size	Indicates the maximum file size (in KB) for each dump file when *replication_dump_strategy*=`auto`. Defaults to 10240KB. If this value is larger than `concerningReplicatedFileSize`, which is set in the `distsearch.conf` file, the value of `concerningReplicatedFileSize` is used instead. KV Store does not pre-calculate the size of the records that will be written to disk, so the size of the resulting files can be affected by the `max_rows_in_memory_per_dump` setting in the `limits.conf` file.
replication_dump_strategy	One of the following two values.

Name	Description
	• `auto`: Default. Dumps are stored in multiple files when the size of the collection exceeds the value of *replication_dump_maximum_file_size*. • `one_file`: Dump files are stored in a single file.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test -d
'accelerated_fields.foo={"a": 1}' -d 'accelerated_fields.bar={"b": -1}' -d "field.a=number" -d
"field.b=cidr"
```

XML Response

```
...
<title>collections-conf</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-09-02T11:50:57-07:00</updated> <generator build="229629" version="6.2"/>

<author>

 <name>Splunk</name>
</author> <link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/> <link
href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/> ... opensearch nodes
elided ... <s:messages/> <entry>

 <title>test</title>
 <id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test</id>
 <updated>2014-09-02T11:50:57-07:00</updated>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="alternate"/>
 <author>
   <name>admin</name>
 </author>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="list"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test/_reload" rel="_reload"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="edit"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="remove"/>
 <link href="/servicesNS/nobody/search/storage/collections/config/test/disable" rel="disable"/>
 <content type="text/xml">
   <s:dict>
     <s:key name="disabled">0</s:key>
     <s:key name="eai:acl"> ... elided ... </s:key>
     <s:key name="eai:appName">search</s:key>
     <s:key name="eai:userName">nobody</s:key>
     <s:key name="accelerated_fields.foo">{"a": 1}
accelerated_fields.bar={"b": -1} field.a=number field.b=cidr</s:key>

     <s:key name="profilingEnabled">false</s:key>
     <s:key name="profilingThresholdMs">100</s:key>
   </s:dict>
 </content>
</entry>
```

storage/collections/data/{collection}

```
https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/data/{collection}
```

Access and manage items of a collection.

DELETE

Delete items in the `{collection}` or delete an entire collection.

Usage details
Use the `query` parameter to specify which entries to delete. If no query is provided, all entries in the collection are deleted.

Request parameters

Name	Type	Description
query	JSON object	Query JSON object. Conditional operators: `$gt`, `$gte`, `$lt`, `$lte`, and `$ne` Logical operators: `$and`, `$or`, and ,`$not` (invert conditional operators) Examples: `query={"title":"Item"}` (Select all documents with property `title` that has value `Item`) `query={"price":{"$gt":5}}` (Select all documents with `price` greater than `5`)

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA -X DELETE
```

XML Response
No values returned.

GET

Access a specific `{collection}`.

Request parameters

Parameter order in the request does not matter. Parameters are always applied in the order of `sort`, `skip`, and `limit`.

Name	Type	Description

Name	Type	Description
fields	String	Comma-separated list of fields to include (1) or exclude (0). A fields value cannot contain both include and exclude specifications except for exclusion of the `_key` field. Examples: `fields=firstname,surname` (Include only `firstname`, `surname`, and `_key` fields) `fields=firstname,surname,_key:0` (Include only the `firstname` and `surname` fields) `fields=address:0` (Include all fields except the `address` field)
shared	Boolean	Defaults to false. Set to true to return records for the specified user as well as records for the `nobody` user.
limit	Number	Maximum number of items to return. For example, to return five items, use `limit=5`.
skip	Number	Number of items to skip from the start. For example, to skip the first ten items, use `skip=10`.
sort	String	Sort order. Examples: `sort=surname` (Sort by `surname`, ascending) `sort=surname,firstname` (Sort by `surname`, ascending, after `firstname`, ascending) `sort=surname:-1,firstname:1` (Sort by `surname`, descending, after `firstname`, ascending `sort=surname:1,first name` (Sort by `surname`, ascending, after `firstname`, ascending
query	JSON object	Query JSON object. Conditional operators: `$gt`, `$gte`, `$lt`, `$lte`, and `$ne` Logical operators: `$and`, `$or`, and ,`$not` (invert conditional operators) Examples: `query={"title":"Item"}` (Select all documents with property `title` that has value `Item`) `query={"price":{"$gt":5}}` (Select all documents with `price` greater than `5`)

Returned values

The response includes a JSON document.

Example

```
[ { "myKey" : "abc", "_user" : "nobody", "_key" : "5410be5441ba15298e4624d1" } ]
```

POST

Insert an item into the `{collection}`.

Usage details

The `Content-Type` header must be `application/json`.

The `_key` is autogenerated, if not manually specified.

Request parameters

Make sure that the item to add is a JSON-formatted document, such as the following example.

```
{ "name": "A" }
```

Returned values

The response includes a JSON-formatted document key, such as the following example.

```
{
    "_key": "530bc62fc9a6577fdf13651f"
}
```

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA -H "Content-Type:
application/json" -d '{ "myKey": "abc",  "myOtherKey": "abcdef"}'
```

XML Response

```
{"_key":"5410be5441ba15298e4624d1"}
```

storage/collections/data/{collection}/{key}

`https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/data/{collection}/{key}`

Access and manage a specific `{key}` item in a `{collection}`.

DELETE

Delete a collection item.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/5410caf041ba15298e4624d6
-X DELETE
```

XML Response

No values returned.

GET

Access a collection item.

Request parameters

None

Returned values

The response includes a JSON-formatted `{key}` document, such as the following example.

```
{"myKey" : "abc", "myOtherKey" : "uvwxyz", "_user" : "nobody", "_key" : "5410c8dc41ba15298e4624d5"}
```

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/5410c8dc41ba15298e4624d5
```

XML Response

```
{ "myKey" : "abc", "myOtherKey" : "uvwxyz", "_user" : "nobody", "_key" : "5410c8dc41ba15298e4624d5" }
```

POST

Update a collection item.

Usage details

The header `Content-Type` must be `application/json`.

Request parameters

Pass in a JSON-formatted document for the `{key}` that you are updating. For example, use `{ "myKey": "fizz"}`.

Returned values

The response includes a JSON-formatted `{key}` such as the following example.

```
{"_key":"5410c8dc41ba15298e4624d5"}
```

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/5410c8dc41ba15298e4624d5
-H "Content-Type: application/json" -d '{ "myKey": "fizz"}'
```

XML Response

```
{"_key":"5410c8dc41ba15298e4624d5"}
```

storage/collections/data/{collection}/batch_find

`https://<host>:<mPort>/servicesNS/storage/collections/data/{collection}/batch_find`
Perform multiple queries in a batch.

POST

Perform multiple queries in a batch.

Request parameters

Pass in the JSON array of queries to run. Parameter order in the request does not matter. Parameters are always applied in the order of `sort`, `skip`, and `limit`.

Name	Type	Description
fields	String	Comma-separated list of fields to include (`1`) or exclude (`0`). A fields value cannot contain both include and exclude specifications except for exclusion of the `_key` field. Examples: `fields=firstname,surname` (Include only `firstname`, `surname`, and `_key` fields) `fields=firstname,surname,_key:0` (Include only the `firstname` and `surname` fields. `fields=address:0` (Include all fields except the `address` field)
shared	Boolean	Defaults to false. Set to true to return records for the specified user as well as records for the `nobody` user.
limit	Number	Maximum number of items to return. For example, to return five items, use `limit=5`.
skip	Number	Number of items to skip from the start. For example, to skip the first ten items, use `skip=10`.
sort	String	Sort order. Examples: `sort=surname` (Sort by `surname`, ascending) `sort=surname,firstname` (Sort by `surname`, ascending, after `firstname`, ascending) `sort=surname:-1,firstname:1` (Sort by `surname`, descending, after `firstname`, ascending `sort=surname:1,first name` (Sort by `surname`, ascending, after `firstname`, ascending
query	JSON object	Query JSON object. Conditional operators: `$gt`, `$gte`, `$lt`, `$lte`, and `$ne` Logical operators: `$and`, `$or`, and ,`$not` (invert conditional operators) Examples: `query={"title":"Item"}` (Select all documents with property `title` that has value `Item`) `query={"price":{"$gt":5}}` (Select all documents with `price` greater than `5`)

Returned values

The response includes a JSON-formatted array of an array of records. The first array of records is the result of the first query, the second array of records is the result of the second query, and so on.

Example request and response

XML Request

```
queries='['
queries+='{"query": {"myKey": "def"}},'
queries+='{"query": {"myKey": "abc"}},'
queries+='{"query": {"myKey": "jkl"}},'
queries+='{"shared": true, "fields": {"myKey": 1}, "sort": [{"myKey": 1}], "limit": 2}'
queries+=']'
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/batch_find -H
"Content-Type: application/json" -d "$queries"
```

XML Response

```
[
  [{"myKey":"def","_user":"nobody","_key":"f3jel0421dsw1024f3fd1a78"}],
  [{"myKey":"abc","_user":"nobody","_key":"b2jcw0405saw1221177aa78f"}],
  [{"myKey":"jkl","_user":"nobody","_key":"3b4b0d9ef63cc83959e5ed77"}],
  [{"myKey":"abc"},{"myKey":"def"}]
]
```

storage/collections/data/{collection}/batch_save

`https://<host>:<mPort>/servicesNS/storage/collections/data/{collection}/batch_save`

Perform multiple save operations in a batch.

POST

Perform multiple save operations in a batch.

Usage details

The request header `Content-Type` must be `application/json`.

If a document does not have a `_key` field or store does not have a matching document ID, a `_key` new document is created.

If an operation fails, the server stops batch processing and returns an HTTP status code other than `200`.

Request parameters

Pass in the JSON array of documents to save.

Returned values

The response includes a JSON-formatted list of keys added, such as the following example.

```
[ "5410c43241ba15298e4624d3", "5418c54e41ba152267763c01" ]
```

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/batch_save -H
"Content-Type: application/json" -d '[{ "_key": "5410c43241ba15298e4624d3", "name": "AAAAAAAA" },{ "name":
```

```
"A" }]'
```

XML Response

```
[ "5410c43241ba15298e4624d3", "5418c54e41ba152267763c01" ]
```

License endpoints

License endpoint descriptions

Manage licensing configurations.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. License endpoints are generally not accessible in Splunk Cloud Platform.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

licenser/groups

`https://<host>:<mPort>/services/licenser/groups`

Provides access to the configuration of licenser groups.

A licenser group contains one or more licenser stacks that can operate concurrently. Only one licenser group is active at any given time.

GET

Lists all licenser groups.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
is_active	Indicates if the license group is active.
stack_ids	The license stacks in the license group.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/groups
```

XML Response

```
...
 <title>groups</title>
 <id>https://localhost:8089/services/licenser/groups</id>
 <updated>2011-07-11T09:45:35-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>Enterprise</title>
   <id>https://localhost:8089/services/licenser/groups/Enterprise</id>
   <updated>2011-07-11T09:45:35-07:00</updated>
   <link href="/services/licenser/groups/Enterprise" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/groups/Enterprise" rel="list"/>
   <link href="/services/licenser/groups/Enterprise" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
       <s:key name="is_active">1</s:key>
       <s:key name="stack_ids">
         <s:list>
           <s:item>enterprise</s:item>
         </s:list>
       </s:key>
     </s:dict>
   </content>
 </entry>
```

licenser/groups/{name}

```
https://<host>:<mPort>/services/licenser/groups/{name}
```

Manage the `{name}` licenser group.

GET

List a specific licenser group.

Usage details
A licenser group contains one or more licenser stacks that can operate concurrently. Only one licenser group is active at any given time.

Request parameters

None

Returned values

Name	Description
is_active	Indicates if the license group is active.
stack_ids	The license stacks in the license group.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/groups/Forwarder
```

XML Response

```
...
 <title>groups</title>
 <id>https://localhost:8089/services/licenser/groups</id>
 <updated>2011-07-11T09:47:18-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>Forwarder</title>
   <id>https://localhost:8089/services/licenser/groups/Forwarder</id>
```

```
    <updated>2011-07-11T09:47:18-07:00</updated>
    <link href="/services/licenser/groups/Forwarder" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/licenser/groups/Forwarder" rel="list"/>
    <link href="/services/licenser/groups/Forwarder" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>is_active</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="is_active">0</s:key>
        <s:key name="stack_ids">
          <s:list>
            <s:item>forwarder</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Activate a specific licenser group and deactivate the previously active one.

Usage details

There can only be a single active licenser group for a given Splunk instance. Use this to switch between, for example, free to enterprise, or download-trial to free.

Request parameters

Name	Type	Default	Description
is_active	Boolean		**Required**. Active specific licenser group

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/groups/Enterprise -d is_active=1
```

XML Response

```
 <title>groups</title>
 <id>https://localhost:8089/services/licenser/groups</id>
 <updated>2011-07-11T09:55:02-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
```

licenser/licenses

```
https://<host>:<mPort>/services/licenser/licenses
```

Provides access to the licenses for this Splunk Enterprise instance.

A license enables various features for a Splunk instance, including but not limited to indexing quota, auth, search, forwarding.

GET

List all licenses added.

Usage details
Only a subset of these licenses may be active however, this is simply listing all licenses in every stack/group, regardless of which group is active.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description

creation_time	The creation time of this license, in Coordinated Universal Time (UTC).
expiration_time	The time this license expires, in Coordinated Universal Time (UTC).
features	The list of features and components enabled by this license.
group_id	The ID of the group to which this license belongs.
label	Plain text description of this license.
license_hash	Unique identifier for the license. The REST API uses this identifier to access this license.
max_violations	The maximum number of violations allowed during the specified window period (`window_period`. Searching is disabled when `max_violations` is exceeded.
quota	Daily indexing quota, in bytes, for this license.
sourcetypes	The list of allowed sourcetypes for this list. You cannot use this license to index sourcetypes that are not present in this list. An empty list indicates all sourcetypes are allowed.
stack_id	The ID of the license stack to which this license belongs.
status	The status of a license can be either VALID or EXPIRED.
type	Provides any additional information about the type of this license.
window_period	The rolling period, in days, in which violations are aggregated.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/licenses
```

XML Response

```
...
<title>licenses</title>
 <id>https://localhost:8089/services/licenser/licenses</id>
 <updated>2011-07-11T09:30:33-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/licenses/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>E08B ... elided ...FA75BF</title>
   <id>https://localhost:8089/services/licenser/licenses/E08B ... elided ...FA75BF</id>
   <updated>2011-07-11T09:30:33-07:00</updated>
   <link href="/services/licenser/licenses/E08B ... elided ...FA75BF" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
```

```
  <link href="/services/licenser/licenses/E08B ... elided ...FA75BF" rel="list"/>
  <link href="/services/licenser/licenses/E08B ... elided ...FA75BF" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="creation_time">1309852804</s:key>
      ... eai:acl node elided ...
      <s:key name="expiration_time">1315641604</s:key>
      <s:key name="features">
        <s:list>
          <s:item>Auth</s:item>
          <s:item>FwdData</s:item>
          <s:item>RcvData</s:item>
          <s:item>LocalSearch</s:item>
          <s:item>DistSearch</s:item>
          <s:item>RcvSearch</s:item>
          <s:item>ScheduledSearch</s:item>
          <s:item>Alerting</s:item>
          <s:item>DeployClient</s:item>
          <s:item>DeployServer</s:item>
          <s:item>SplunkWeb</s:item>
          <s:item>SigningProcessor</s:item>
          <s:item>SyslogOutputProcessor</s:item>
          <s:item>AllowDuplicateKeys</s:item>
        </s:list>
      </s:key>
      <s:key name="group_id">Trial</s:key>
      <s:key name="label">Splunk Enterprise Download Trial</s:key>
      <s:key name="license_hash">E08B ... elided ...FA75BF</s:key>
      <s:key name="max_violations">5</s:key>
      <s:key name="quota">524288000</s:key>
      <s:key name="sourcetypes">
        <s:list/>
      </s:key>
      <s:key name="stack_id">download-trial</s:key>
      <s:key name="status">VALID</s:key>
      <s:key name="type">download-trial</s:key>
      <s:key name="window_period">30</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Add a license entitlement to the current instance.

Request parameters

Name	Type	Default	Description
name	string		**Required**. Path to license file on server. If the payload parameter is specified, the name parameter is ignored.
payload	string		String representation of license, encoded in xml

Returned values

Name	Description
creation_time	The creation time of this license, in Coordinated Universal Time (UTC).
expiration_time	The time this license expires, in Coordinated Universal Time (UTC).
features	The list of features and components enabled by this license.
group_id	The ID of the group to which this license belongs.
label	Plain text description of this license.
license_hash	Unique identifier for the license. The REST API uses this identifier to access this license.
max_violations	The maximum number of violations allowed during the specified window period (`window_period`. Searching is disabled when `max_violations` is exceeded.
payload	String representation of license, encoded in xml.
quota	Daily indexing quota, in bytes, for this license.
sourcetypes	The list of allowed sourcetypes for this list. You cannot use this license to index sourcetypes that are not present in this list. An empty list indicates all sourcetypes are allowed.
stack_id	The ID of the license stack to which this license belongs.
status	The status of a license can be either VALID or EXPIRED.
type	Provides any additional information about the type of this license.
window_period	The rolling period, in days, in which violations are aggregated.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/licenses -d
name=/Users/myusername/downloads/Splunk_enterprise.lic
```

XML Response

```
...
 <title>licenses</title>
 <id>https://localhost:8089/services/licenser/licenses</id>
 <updated>2011-07-11T09:41:32-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/licenses/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>CF6C50 ... elided ...72CE6C</title>
   <id>https://localhost:8089/services/licenser/licenses/CF6C50 ... elided ...72CE6C</id>
   <updated>2011-07-11T09:41:32-07:00</updated>
```

```
    <link href="/services/licenser/licenses/CF6C50 ... elided ...72CE6C" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/licenser/licenses/CF6C50 ... elided ...72CE6C" rel="list"/>
    <link href="/services/licenser/licenses/CF6C50 ... elided ...72CE6C" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="creation_time">1306168427</s:key>
        ... eai:acl node elided ...
        <s:key name="expiration_time">2147483647</s:key>
        <s:key name="features">
          <s:list>
            <s:item>Auth</s:item>
            <s:item>FwdData</s:item>
            <s:item>RcvData</s:item>
            <s:item>LocalSearch</s:item>
            <s:item>DistSearch</s:item>
            <s:item>RcvSearch</s:item>
            <s:item>ScheduledSearch</s:item>
            <s:item>Alerting</s:item>
            <s:item>DeployClient</s:item>
            <s:item>DeployServer</s:item>
            <s:item>SplunkWeb</s:item>
            <s:item>SigningProcessor</s:item>
            <s:item>SyslogOutputProcessor</s:item>
            <s:item>CanBeRemoteManager</s:item>
          </s:list>
        </s:key>
        <s:key name="group_id">Enterprise</s:key>
        <s:key name="label">Splunk Enterprise</s:key>
        <s:key name="license_hash">CF6C50 ... elided ...72CE6C</s:key>
        <s:key name="max_violations">5</s:key>
        <s:key name="quota">10737418240</s:key>
        <s:key name="sourcetypes">
          <s:list/>
        </s:key>
        <s:key name="stack_id">enterprise</s:key>
        <s:key name="status">VALID</s:key>
        <s:key name="type">enterprise</s:key>
        <s:key name="window_period">30</s:key>
      </s:dict>
    </content>
  </entry>
```

licenser/licenses/{name}

`https://<host>:<mPort>/services/licenser/licenses/{name}`
Access or delete the `{name}` license.

DELETE

Delete the license with a hash corresponding to `{name}`

Usage details

You cannot delete the last license out of an active group. First, deactivate the group (by switching to another group) and then perform the delete.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/services/licenser/licenses/E4BF ... elided
...FC639D
```

XML Response

```
...
 <title>licenses</title>
 <id>https://localhost:8089/services/licenser/licenses</id>
 <updated>2011-07-07T09:45:12-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/licenses/_new" rel="create"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

GET

List license details.

Usage details

The `{name}` portion of URL is the hash of the license payload.

Request parameters

None

Returned values

Name	Description
creation_time	The creation time of this license, in Coordinated Universal Time (UTC).
expiration_time	The time this license expires, in Coordinated Universal Time (UTC).
features	The list of features and components enabled by this license.
group_id	The ID of the group to which this license belongs.
label	Plain text description of this license.
license_hash	Unique identifier for the license. The REST API uses this identifier to access this license.
max_violations	The maximum number of violations allowed during the specified window period (`window_period`. Searching is disabled when `max_violations` is exceeded.
quota	Daily indexing quota, in bytes, for this license.
sourcetypes	The list of allowed sourcetypes for this list. You cannot use this license to index sourcetypes that are not present in this list. An empty list indicates all sourcetypes are allowed.
stack_id	The ID of the license stack to which this license belongs.
status	The status of a license can be either VALID or EXPIRED.
type	Provides any additional information about the type of this license.
window_period	The rolling period, in days, in which violations are aggregated.

Example request and response

XML Request

```
curl -k -u admin:pass https://127.0.0.1:3339/services/licenser/licenses/E4BF ... elided ...FC639D
```

XML Response

```
...
<title>licenses</title>
 <id>https://localhost:8089/services/licenser/licenses</id>
 <updated>2011-07-05T15:57:08-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/licenses/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>E4BF ... elided ...FC639D</title>
   <id>https://localhost:8089/services/licenser/licenses/E4BF ... elided ...FC639D</id>
   <updated>2011-07-05T15:57:08-07:00</updated>
```

```
  <link href="/services/licenser/licenses/E4BF ... elided ...FC639D" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/licenser/licenses/E4BF ... elided ...FC639D" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="creation_time">1300901512</s:key>
      <s:key name="eai:acl"> ... elided ...</s:key>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list/>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="expiration_time">1314811912</s:key>
      <s:key name="features">
        <s:list>
          <s:item>Auth</s:item>
          <s:item>FwdData</s:item>
          <s:item>RcvData</s:item>
          <s:item>LocalSearch</s:item>
          <s:item>DistSearch</s:item>
          <s:item>RcvSearch</s:item>
          <s:item>ScheduledSearch</s:item>
          <s:item>Alerting</s:item>
          <s:item>DeployClient</s:item>
          <s:item>DeployServer</s:item>
          <s:item>SplunkWeb</s:item>
          <s:item>SigningProcessor</s:item>
          <s:item>SyslogOutputProcessor</s:item>
          <s:item>AllowDuplicateKeys</s:item>
          <s:item>CanBeRemoteManager</s:item>
        </s:list>
      </s:key>
      <s:key name="group_id">Enterprise</s:key>
      <s:key name="label">Splunk Internal License</s:key>
      <s:key name="license_hash">E4BF ... elided ...FC639D</s:key>
      <s:key name="max_violations">5</s:key>
      <s:key name="quota">10737418240</s:key>
      <s:key name="sourcetypes"><s:list/></s:key>
      <s:key name="stack_id">enterprise</s:key>
      <s:key name="status">VALID</s:key>
      <s:key name="type">enterprise</s:key>
      <s:key name="window_period">30</s:key>
    </s:dict>
  </content>
</entry>
```

licenser/localpeer

`https://<host>:<mPort>/services/licenser/localpeer`

Get license state information for the Splunk instance.

GET

Get license state information for the Splunk instance.

Request parameters

None

Returned values

Name	Description
add_ons	List of add-ons resident on this instance, and add-on parameters.
connection_timeout	Instance connection timeout (seconds).
features	List of key-value pairs of the following features and their ENABLED/DISABLED status: • Acceleration • AdvancedSearchCommands • AdvancedXML • Alerting • AllowDuplicateKeys • Auth • CanBeRemoteManager • CustomRoles • DeployClient • DeployServer • DistSearch • FwdData • GuestPass • KVStore • LDAPAuth • LocalSearch • MultisiteClustering • NontableLookups • RcvData • RcvSearch • ResetWarnings">DISABLED_DUE_TO_LICENSE</s:key> • RollingWindowAlerts • ScheduledAlerts • ScheduledReports • ScheduledSearch • SearchheadPooling • SigningProcessor • SplunkWeb • SyslogOutputProcessor • UnisiteClustering
last_manager_contact_attempt_time	Time of last attempt to contact manager.
last_manager_contact_success_time	Time of last successful attempt to contact manager.

Name	Description
last_trackerdb_service_time	Time of last license servicing, tracking persistent store.
license_keys	List of license keys this instance is using.
manager_guid	Manager license GUID.
manager_uri	Manager license URI.
receive_timeout	Network layer receive timeout for communication to manager (seconds).
send_timeout	Network layer send timeout for communication to manager (seconds).
peer_id	This instance GUID.
peer_label	This instance server name.
squash_threshold	Threshold that enables source/host squashing of rows of usage data sent to manager periodically.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/localpeer
```

XML Response

```
...
 <title>localpeer</title>
 <id>https://localhost:8089/services/licenser/localpeer</id>
 <updated>2014-09-08T11:30:21-07:00</updated>
 <generator build="221120" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>license</title>
   <id>https://localhost:8089/services/licenser/localpeer/license</id>
   <updated>2014-09-08T11:30:21-07:00</updated>
   <link href="/services/licenser/localpeer/license" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/localpeer/license" rel="list"/>
   <link href="/services/licenser/localpeer/license" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="add_ons">
         <s:dict>
           <s:key name="hadoop">
             <s:dict>
               <s:key name="parameters">
                 <s:dict>
                   <s:key name="erp_type">report</s:key>
                   <s:key name="maxNodes">10</s:key>
```

```
                </s:dict>
              </s:key>
              <s:key name="type">external_results_provider</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="connection_timeout">30</s:key>
      <s:key name="eai:acl"> ... elided ... </s:key>
      <s:key name="features">
        <s:dict>
          <s:key name="Acceleration">ENABLED</s:key>
          <s:key name="AdvancedSearchCommands">ENABLED</s:key>
          <s:key name="AdvancedXML">ENABLED</s:key>
          <s:key name="Alerting">ENABLED</s:key>
          <s:key name="AllowDuplicateKeys">ENABLED</s:key>
          <s:key name="Auth">ENABLED</s:key>
          <s:key name="CanBeRemoteManager">ENABLED</s:key>
          <s:key name="CustomRoles">ENABLED</s:key>
          <s:key name="DeployClient">ENABLED</s:key>
          <s:key name="DeployServer">ENABLED</s:key>
          <s:key name="DistSearch">ENABLED</s:key>
          <s:key name="FwdData">ENABLED</s:key>
          <s:key name="GuestPass">ENABLED</s:key>
          <s:key name="KVStore">ENABLED</s:key>
          <s:key name="LDAPAuth">ENABLED</s:key>
          <s:key name="LocalSearch">ENABLED</s:key>
          <s:key name="MultisiteClustering">ENABLED</s:key>
          <s:key name="NontableLookups">ENABLED</s:key>
          <s:key name="RcvData">ENABLED</s:key>
          <s:key name="RcvSearch">ENABLED</s:key>
          <s:key name="ResetWarnings">DISABLED_DUE_TO_LICENSE</s:key>
          <s:key name="RollingWindowAlerts">ENABLED</s:key>
          <s:key name="ScheduledAlerts">ENABLED</s:key>
          <s:key name="ScheduledReports">ENABLED</s:key>
          <s:key name="ScheduledSearch">ENABLED</s:key>
          <s:key name="SearchheadPooling">ENABLED</s:key>
          <s:key name="SigningProcessor">ENABLED</s:key>
          <s:key name="SplunkWeb">ENABLED</s:key>
          <s:key name="SyslogOutputProcessor">ENABLED</s:key>
          <s:key name="UnisiteClustering">ENABLED</s:key>
        </s:dict>
      </s:key>
      <s:key name="last_manager_contact_attempt_time">1410201013</s:key>
      <s:key name="last_manager_contact_success_time">1410201013</s:key>
      <s:key name="last_trackerdb_service_time">0</s:key>
      <s:key name="license_keys">
        <s:list>
          <s:item>4467A79214BACAD9BB01F28193D6E15129DADC3B99D69D78884D4D68D2DDE750</s:item>
        </s:list>
      </s:key>
      <s:key name="manager_guid">9CBD8473-4E7D-4FF2-A042-050C5C27C298</s:key>
      <s:key name="manager_uri">self</s:key>
      <s:key name="receive_timeout">30</s:key>
      <s:key name="send_timeout">30</s:key>
      <s:key name="peer_id">9CBD8473-4E7D-4FF2-A042-050C5C27C298</s:key>
      <s:key name="peer_label">MY MACHINE</s:key>
      <s:key name="squash_threshold">2000</s:key>
    </s:dict>
  </content>
</entry>
```

licenser/messages

`https://<host>:<mPort>/services/licenser/messages`

Access licenser messages.

Messages may range from helpful warnings about being close to violations, licenses expiring or more severe alerts regarding overages and exceeding license warning window.

GET

List all messages/alerts/persisted warnings for this node.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
category	Indicates the category for the licenser message. The category can be any of the following: license_window pool_over_quota stack_over_quota orphan_peer pool_warning_count pool_violated_peer_count
create_time	The time the message was created in the system, expressed in Coordinated Universal time (UTC).
description	The actual licenser message that is displayed.
pool_id	The ID of the licesne pool to which the message applies. If a pool ID is not present, then the message in not applicable to a specific license pool.
severity	Indicates the severity of the message. The severity can be any of the following: INFO WARN ERROR

Name	Description
peer_id	The ID of the license peer to which the message applies.
stack_id	The ID of the license stack to which the message applies. If a stack ID is not present, thae the message is not applicable to a specific license stack.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/messages
```

XML Response

```
...
 <title>licensermessages</title>
 <id>https://localhost:8089/services/licenser/messages</id>
 <updated>2011-08-02T03:50:46-07:00</updated>
 <generator version="105103"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>70a19a5cfe6d7c2a678089638dee7bea</title>
   <id>https://localhost:8089/services/licenser/messages/70a19a5cfe6d7c2a678089638dee7bea</id>
   <updated>2011-08-02T03:50:46-07:00</updated>
   <link href="/services/licenser/messages/70a19a5cfe6d7c2a678089638dee7bea" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/messages/70a19a5cfe6d7c2a678089638dee7bea" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="category">pool_warning_count</s:key>
       <s:key name="create_time">1312282230</s:key>
       <s:key name="description">This pool contains peer(s) with 3 warnings</s:key>
       ... eai:acl node elided ...
       <s:key name="pool_id"/>
       <s:key name="severity">WARN</s:key>
       <s:key name="peer_id"/>
       <s:key name="stack_id"/>
     </s:dict>
   </content>
 </entry>
```

licenser/messages/{name}

```
https://<host>:<mPort>/services/licenser/messages/{name}
```

Get the message with message ID `{name}`.

GET

List specific message whose msgId corresponds to {name} component.

Request parameters

None

Returned values

Name	Description
category	Indicates the category for the licenser message. The category can be any of the following: license_window pool_over_quota stack_over_quota orphan_peer pool_warning_count pool_violated_peer_count
create_time	The time the message was created in the system, expressed in Coordinated Universal time (UTC).
description	The actual licenser message that is displayed.
pool_id	The ID of the licesne pool to which the message applies. If a pool ID is not present, then the message in not applicable to a specific license pool.
severity	Indicates the severity of the message. The severity can be any of the following: INFO WARN ERROR
peer_id	The ID of the license peer to which the message applies.
stack_id	The ID of the license stack to which the message applies. If a stack ID is not present, thae the message is not applicable to a specific license stack.

Example request and response

XML Request

```
curl -k -u admin:pass https://127.0.0.1:3339/services/licenser/messages/2702b33a1bd369ae9209a9ecf4cb39db
```

XML Response

```
...
  <title>licensermessages</title>
   <id>https://127.0.0.1:3339/services/licenser/messages</id>
   <updated>2011-05-16T21:45:17-07:00</updated>
   <generator version="99678"/>
   <author>
       <name>Splunk</name>
   </author>
   <opensearch:totalResults>1</opensearch:totalResults>
   <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
   <opensearch:startIndex>0</opensearch:startIndex>
   <s:messages/>
   <entry>
       <title>2702b33a1bd369ae9209a9ecf4cb39db</title>
       <id>https://127.0.0.1:3339/services/licenser/messages/2702b33a1bd369ae9209a9ecf4cb39db</id>
       <updated>2011-05-16T21:45:17-07:00</updated>
       <link href="/services/licenser/messages/2702b33a1bd369ae9209a9ecf4cb39db" rel="alternate"/>
       <author>
           <name>system</name>
       </author>
       <link href="/services/licenser/messages/2702b33a1bd369ae9209a9ecf4cb39db" rel="list"/>
       <content type="text/xml">
           <s:dict>
               <s:key name="category">license_window</s:key>
               <s:key name="create_time">1305607136</s:key>
               <s:key name="description">test warnings</s:key>
               <s:key name="eai:acl">... elided ...</s:key>
               <s:key name="eai:attributes">
                   <s:dict>
                       <s:key name="optionalFields">
                           <s:list/>
                       </s:key>
                       <s:key name="requiredFields">
                           <s:list/>
                       </s:key>
                       <s:key name="wildcardFields">
                           <s:list/>
                       </s:key>
                   </s:dict>
               </s:key>
               <s:key name="pool_id"/>
               <s:key name="severity">WARN</s:key>
               <s:key name="peer_id"/>
               <s:key name="stack_id"/>
           </s:dict>
       </content>
   </entry>
```

licenser/pools

```
https://<host>:<mPort>/services/licenser/pools
```

Access the licenser pools configuration.

A pool logically partitions the daily volume entitlements of a stack. You can use a license pool to divide license privileges amongst multiple peers.

GET

Enumerate all pools.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
description	Description of the license pool.
quota	The byte quota of this license pool. MAX: maximum amount allowed by the license. You can only have one pool with MAX size in a stack. Number: the number of bytes allowed by this license.
peers	peerids that are members of this pool. Returned as a list in Atom format. See example below.
peers_usage_bytes	Usage, in bytes, of peers to this license.
stack_id	Stack ID of the stack corresponding to this pool.
used_bytes	Usage, in bytes, for this license pool.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/pools
```

XML Response

```
 <title>pools</title>
 <id>https://localhost:8089/services/licenser/pools</id>
 <updated>2011-07-08T10:55:18-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/pools/_new" rel="create"/>
 <link href="/services/licenser/pools/_reload" rel="_reload"/>
 <opensearch:totalResults>4</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 ... elided ...
 <entry>
   <title>auto_generated_pool_enterprise</title>
   <id>https://localhost:8089/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise</id>
   <updated>2011-07-08T10:55:18-07:00</updated>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="list"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="edit"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="description">auto_generated_pool_enterprise</s:key>
       <s:key name="eai:acl"> ... elided ...</s:key>
       <s:key name="quota">MAX</s:key>
       <s:key name="peers"><s:list><s:item>*</s:item></s:list></s:key>
       <s:key name="peers_usage_bytes">
         <s:dict><s:key name="1F3A34AE-75DA-4680-B184-5BF309843919">26445659</s:key></s:dict>
       </s:key>
       <s:key name="stack_id">enterprise</s:key>
       <s:key name="used_bytes">26445659</s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>auto_generated_pool_forwarder</title>
   <id>https://localhost:8089/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder</id>
   <updated>2011-07-08T10:55:18-07:00</updated>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="list"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="edit"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="description">auto_generated_pool_forwarder</s:key>
      <s:key name="eai:acl"> ... elided ...</s:key>
       <s:key name="quota">MAX</s:key>
       <s:key name="peers"><s:list><s:item>*</s:item></s:list></s:key>
       <s:key name="peers_usage_bytes"></s:key>
       <s:key name="stack_id">forwarder</s:key>
       <s:key name="used_bytes">0</s:key>
     </s:dict>
   </content>
 </entry>
 ... elided ...
```

POST

Create a license pool.

Request parameters

description	String		Description of this pool
Name	**Type**	**Default**	**Description**
name	String		**Required**. The name of the license pool you are creating.
quota	String		**Required**. Defines the byte quota of this pool. Valid values: MAX: maximum amount allowed by the license. You can only have one pool with MAX size in a stack. Number[MB|GB]: Specify a specific size. For example, 552428800, or simply specify 50MB.
peers	String		Comma-separated list of peerids that are members of this pool, or '*' to accept all peers. You can also specify a comma-separated list of guids to specify peers that can connect to this pool.
stack_id	Enum		**Required**. Valid values: (download-trial | Enterprise | Forwarder | Free | Lite | Lite_Free) Stack ID of the stack corresponding to this pool

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/pools -d name=myLicensePool -d quota=MAX -d
peers=* -d stack_id=enterprise
```

XML Response

```
...
 <title>pools</title>
 <id>https://localhost:8089/services/licenser/pools</id>
 <updated>2011-07-08T11:31:47-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/pools/_new" rel="create"/>
 <link href="/services/licenser/pools/_reload" rel="_reload"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

licenser/pools/{name}

`https://<host>:<mPort>/services/licenser/pools/{name}`

Manage the `{name}` license pool.

DELETE

Delete the specified pool.

Usage details
Deleting pools is not supported for every pool. Certain stacks have fixed pools which cannot be deleted.

Request parameters
None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/licenser/pools/auto_generated_pool_enterprise
```

XML Response

```
...
 <title>pools</title>
 <id>https://localhost:8089/services/licenser/pools</id>
 <updated>2011-07-08T11:29:26-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/pools/_new" rel="create"/>
 <link href="/services/licenser/pools/_reload" rel="_reload"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

GET

Lists details of the pool specified by {name}.

Request parameters

None

Returned values

Name	Description
description	Description of the license pool.
quota	The byte quota of this license pool. MAX: maximum amount allowed by the license. You can only have one pool with MAX size in a stack. Number: the number of bytes allowed by this license.
peers	peerids that are members of this pool. Returned as a list in Atom format. See example below.
peers_usage_bytes	Usage, in bytes, of peers to this license.
stack_id	Stack ID of the stack corresponding to this pool.
used_bytes	Usage, in bytes, for this license pool.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/pools/auto_generated_pool_forwarder
```

XML Response

```
...
<title>pools</title>
 <id>https://localhost:8089/services/licenser/pools</id>
 <updated>2011-07-08T11:03:37-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/pools/_new" rel="create"/>
 <link href="/services/licenser/pools/_reload" rel="_reload"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>auto_generated_pool_forwarder</title>
   <id>https://localhost:8089/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder</id>
   <updated>2011-07-08T11:03:37-07:00</updated>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="list"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="edit"/>
   <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="description">auto_generated_pool_forwarder</s:key>
       <s:key name="eai:acl"> ... elided ...</s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list>
               <s:item>append_peers</s:item>
               <s:item>description</s:item>
               <s:item>quota</s:item>
               <s:item>peers</s:item>
             </s:list>
           </s:key>
           <s:key name="requiredFields">
             <s:list/></s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="quota">MAX</s:key>
       <s:key name="peers"><s:list><s:item>*</s:item></s:list></s:key>
       <s:key name="peers_usage_bytes"></s:key>
       <s:key name="stack_id">forwarder</s:key>
       <s:key name="used_bytes">0</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Edit properties of the pool specified by {name}.

Request parameters

Name	Type	Default	Description
append_peers	Boolean		Flag which controls whether newly specified peers is appended to existing peers list or overwritten
description	String		Description of this pool
quota	String		Defines the byte quota of this pool. Valid values: MAX: maximum amount allowed by the license. You can only have one pool with MAX size in a stack. Number[MB|GB]: Specify a specific size. For example, 552428800, or simply specify 50MB.
peers	String		Comma-separated list of peerids that are members of this pool, or '*' to accept all peers. You can also specify a comma-separated list of guids to specify peers that can connect to this pool.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/pools/myLicensePool -d quota=50MB
```

XML Response

```
  ... elided ...
 <entry>
   <title>myLicensePool</title>
   <id>https://localhost:8085/servicesNS/nobody/system/licenser/pools/myLicensePool</id>
   <updated>2011-07-24T08:46:49-07:00</updated>
   <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="list"/>
   <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="edit"/>
   <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="description"></s:key>
       ... eai:acl node elided ...
       <s:key name="eai:attributes">
```

```
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>append_peers</s:item>
              <s:item>description</s:item>
              <s:item>quota</s:item>
              <s:item>peers</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list/></s:key>
          <s:key name="wildcardFields">
            <s:list/></s:key>
        </s:dict>
      </s:key>
      <s:key name="quota">552428800</s:key>
      <s:key name="peers"><s:list><s:item>*</s:item></s:list></s:key>
      <s:key name="peers_usage_bytes">
        <s:dict>
          <s:key name="1F3A34AE-75DA-4680-B184-5BF309843919">39846322</s:key>
        </s:dict>
      </s:key>
      <s:key name="stack_id">enterprise</s:key>
      <s:key name="used_bytes">39846322</s:key>
    </s:dict>
  </content>
</entry>
```

licenser/peers

```
https://<host>:<mPort>/services/licenser/peers
```

Access license peer instances.

GET

List all peers registered to this license manager.

Request parameters

Returned values

Name	Description
label	Plain text name for the license peer.
pool_ids	License pools for which this license peer is a member.
stack_ids	License stacks for which this license peer is a member.
warning_count	Number of license warnings issued for this license peer.

Name	Description

Usage details

Any license peer manager connection attempt is reported regardless of whether it is allocated to a manager licenser pool.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/peers
```

XML Response

```
<title>peers</title>
 <id>https://localhost:8089/services/licenser/peers</id>
 <updated>2011-05-17T09:37:54-07:00</updated>
 <generator version="99849"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>74A43C7E-C33C-41F6-B027-E603D2C3FE68</title>
   <id>https://localhost:8089/servicesNS/nobody/system/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68<
/id>
   <updated>2011-05-17T09:37:54-07:00</updated>
   <link href="/servicesNS/nobody/system/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68"
rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">system</s:key>
           <s:key name="can_write">1</s:key>
             <s:key name="modifiable">0</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                 </s:list>
               </s:key>
```

```
            </s:dict>
          </s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="label">thething-vishalp</s:key>
      <s:key name="pool_ids">
        <s:list>
          <s:item>auto_generated_pool_enterprise</s:item>
          <s:item>auto_generated_pool_forwarder</s:item>
          <s:item>auto_generated_pool_free</s:item>
        </s:list>
      </s:key>
      <s:key name="stack_ids">
        <s:list>
          <s:item>enterprise</s:item>
          <s:item>forwarder</s:item>
          <s:item>free</s:item>
        </s:list>
      </s:key>
      <s:key name="warning_count">0</s:key>
    </s:dict>
  </content>
</entry>
```

licenser/peers/{name}

`https://<host>:<mPort>/services/licenser/peers/{name}`

Get `{name}` licenser peer license information.

GET

List attributes of the peer instance specified by {name}.

Request parameters

None

Returned values

Name	Description
label	Plain text name for the license peer.
pool_ids	License pools for which this license peer is a member.
stack_ids	License stacks for which this license peer is a member.
warning_count	Number of license warnings issued for this license peer.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68
```

XML Response

```
...
<title>peers</title>
 <id>https://127.0.0.1:8282/services/licenser/peers</id>
 <updated>2011-05-17T09:44:10-07:00</updated>
 <generator version="99849"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>74A43C7E-C33C-41F6-B027-E603D2C3FE68</title>
   <id>https://127.0.0.1:8282/servicesNS/nobody/system/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68<
/id>
   <updated>2011-05-17T09:44:10-07:00</updated>
   <link href="/servicesNS/nobody/system/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68"
rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/licenser/peers/74A43C7E-C33C-41F6-B027-E603D2C3FE68" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">system</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list/>
```

```
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="label">thething-vishalp</s:key>
      <s:key name="pool_ids">
        <s:list>
          <s:item>auto_generated_pool_enterprise</s:item>
          <s:item>auto_generated_pool_forwarder</s:item>
          <s:item>auto_generated_pool_free</s:item>
        </s:list>
      </s:key>
      <s:key name="stack_ids">
        <s:list>
          <s:item>enterprise</s:item>
          <s:item>forwarder</s:item>
          <s:item>free</s:item>
        </s:list>
      </s:key>
      <s:key name="warning_count">0</s:key>
    </s:dict>
  </content>
</entry>
```

licenser/stacks

```
https://<host>:<mPort>/services/licenser/stacks
```

Provides access to the license stack configuration.

A license stack is comprised of one or more licenses of the same "type". The daily indexing quota of a license stack is additive, so a stack represents the aggregate entitlement for a collection of licenses.

GET

Enumerate all license stacks.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
label	The name of this license stack.
quota	The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the license stack.

Name	Description
type	Any additional information about the type of this license stack.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/stacks
```

XML Response

```
<title>stacks</title>
 <id>https://localhost:8089/services/licenser/stacks</id>
 <updated>2011-07-08T10:37:33-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>4</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>download-trial</title>
   <id>https://localhost:8089/services/licenser/stacks/download-trial</id>
   <updated>2011-07-08T10:37:33-07:00</updated>
   <link href="/services/licenser/stacks/download-trial" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/stacks/download-trial" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">... elided ...</s:key>
       <s:key name="label">Splunk Enterprise Download Trial</s:key>
       <s:key name="quota">524288000</s:key>
       <s:key name="type">download-trial</s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>enterprise</title>
   <id>https://localhost:8089/services/licenser/stacks/enterprise</id>
   <updated>2011-07-08T10:37:33-07:00</updated>
   <link href="/services/licenser/stacks/enterprise" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/stacks/enterprise" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">... elided ...</s:key>
       <s:key name="label">Splunk Internal License</s:key>
       <s:key name="quota">10737418240</s:key>
       <s:key name="type">enterprise</s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>forwarder</title>
   <id>https://localhost:8089/services/licenser/stacks/forwarder</id>
   <updated>2011-07-08T10:37:33-07:00</updated>
   <link href="/services/licenser/stacks/forwarder" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/stacks/forwarder" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">... elided ...</s:key>
       <s:key name="label">Splunk Forwarder</s:key>
       <s:key name="quota">1048576</s:key>
       <s:key name="type">forwarder</s:key>
     </s:dict>
   </content>
 </entry>
 <entry>
   <title>free</title>
   <id>https://localhost:8089/services/licenser/stacks/free</id>
   <updated>2011-07-08T10:37:33-07:00</updated>
   <link href="/services/licenser/stacks/free" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/stacks/free" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">... elided ...</s:key>
       <s:key name="label">Splunk Free</s:key>
       <s:key name="quota">524288000</s:key>
       <s:key name="type">free</s:key>
     </s:dict>
   </content>
 </entry>
```

licenser/stacks/{name}

`https://<host>:<mPort>/services/licenser/stacks/{name}`

Get `{name}` license stack information.

GET

Retrieve details of a specific license stack.

Usage details

A license stack is comprised of one or more licenses of the same "type". The daily indexing quota of a license stack is additive, so a stack represents the aggregate entitlement for a collection of licenses.

Request parameters

None

Returned values

Name	Description
label	The name of this license stack.
quota	The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the license stack.
type	Any additional information about the type of this license stack.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/enterprise
```

XML Response

```
<title>stacks</title>
 <id>https://localhost:8089/services/licenser/stacks</id>
 <updated>2011-07-08T10:42:44-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>enterprise</title>
   <id>https://localhost:8089/services/licenser/stacks/enterprise</id>
   <updated>2011-07-08T10:42:44-07:00</updated>
   <link href="/services/licenser/stacks/enterprise" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/stacks/enterprise" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app"></s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">0</s:key>
           <s:key name="owner">system</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>admin</s:item>
                   </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>admin</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="sharing">system</s:key>
         </s:dict>
       </s:key>
       <s:key name="eai:attributes"> ... elided ...</s:key>
       <s:key name="label">Splunk Internal License</s:key>
       <s:key name="quota">10737418240</s:key>
       <s:key name="type">enterprise</s:key>
     </s:dict>
   </content>
 </entry>
```

licenser/usage

```
https://<host>:<mPort>/services/licenser/usage
```

Get current license usage stats from the last minute, since midnight server time.

GET

Enumerate license usage information from the last minute, since midnight server time.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
quota	The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the active license group.
peers_usage_bytes	Peer usage bytes across all pools that are within the active license group.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/usage
```

XML Response

```
  <title>licenseusage</title>
  <id>https://localhost:8089/services/licenser/usage</id>
  <updated>2015-06-03T11:46:10-07:00</updated>
  <generator build="6cfc0237739f" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/licenser/usage/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>license_usage</title>
    <id>https://localhost:8089/services/licenser/usage/license_usage</id>
    <updated>2015-06-03T11:46:10-07:00</updated>
    <link href="/services/licenser/usage/license_usage" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/licenser/usage/license_usage" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="quota">214748364800</s:key>
        <s:key name="peers_usage_bytes">0</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

Metrics Catalog endpoints

Metrics Catalog endpoint descriptions

Use the Metrics Catalog REST API to enumerate metrics and the dimensions and dimension values associated with metrics.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication are required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints, and must have the `list_metrics_catalog` **capability** to use the Metrics Catalog endpoint. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings > Access controls > Users**. To determine the capabilities assigned to a role, select **Settings > Access controls > Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Default indexes for Metrics Catalog endpoints

If no metric indexes are defined with the `filter` parameter, Metrics Catalog endpoints use the default indexes specified for the role of the user. To review or update the default indexes for specific roles, select **Settings > Access controls > Roles**, select a role, and review or update the **Indexes searched by default** field.

If the set of default indexes for a role includes a mix of metrics indexes and event indexes, the Metrics Catalog endpoints only use the metrics indexes.

If there are no metrics indexes, the Metrics Catalog endpoints display an empty list.

Splunk Cloud Platform URL for REST API access

Splunk Cloud Platform has a different host and management port syntax than Splunk Enterprise. Use the following URL for Splunk Cloud Platform deployments. If necessary, submit a support case using the Splunk Support Portal to open port 8089 on your deployment.

```
https://<deployment-name>.splunkcloud.com:8089
```

Free trial Splunk Cloud Platform accounts cannot access the REST API.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

catalog/metricstore/metrics

```
https://<host>:<mPort>/services/catalog/metricstore/metrics
```

Use this endpoint to list metric names.

GET

Returns metric names.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Type	Description
earliest	String	Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is `-1d`.
filter	String	Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as index or dimension. For example, to specify a dimension named `app`, use `filter=app`. To specify two index names and values such as `index=index1` and `index=index2`, use `index%3dindex1%26index%3dindex2`.
latest	String	Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is `now`.
list_indexes	Boolean	Optional. When set to `true`, the endpoint returns the index or indexes associated with each metric. The default value is `false`.

Returned values

There are no returned values other than the metric names.

Example request and response

XML Request

List all metric names:

```
curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/metrics
```

XML Response

```
...
  <title>metricstore-metrics</title>
  <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/metrics</id>
  <updated>2017-12-19T19:11:49+00:00</updated>
  <generator build="31fcdba9ddc1" version="7.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/catalog/metricstore/metrics/_acl" rel="_acl"/>
  <opensearch:totalResults>16</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>aws.ec2.CPUUtilization</title>
    <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/metrics
/aws.ec2.CPUUtilization</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/catalog/metricstore/metrics/aws.ec2.CPUUtilization" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/catalog/metricstore/metrics/aws.ec2.CPUUtilization" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">0</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>bbuser</s:item>
                    <s:item>cat_read</s:item>
                    <s:item>power</s:item>
                    <s:item>splunk-system-role</s:item>
                    <s:item>statsd</s:item>
                    <s:item>user</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
```

Example requests

- List all metric names that include the dimension field `dc`:

```
curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/metrics?filter=dc
```

- List all metric names that include either `dc=east` or `dc=west` dimension fields:

```
curl -k -u admin:passwd
https://localhost:8089/services/catalog/metricstore/metrics?filter=dc%3deast&filter=dc%3dwest
```

- List all metric names that are in `index1` or `index2` by their index:

```
curl -k -u admin:passwd
https://localhost:8089/services/catalog/metricstore/metrics?filter=index%3dindex1%26index%3dindex2&list
_indexes=t
```

catalog/metricstore/dimensions

```
https://<host>:<mPort>/services/catalog/metricstore/dimensions
```

Use this endpoint to list dimension names.

GET

Returns dimension names for a given metric.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Type	Description
earliest	String	Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is `-1d`.
filter	String	Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as index or dimension. For example, to specify a dimension named `os`, use `filter=os`. To specify two index names and values such as`index=index1` and `index=index2`, use `index%3dindex1%26index%3dindex2`.
latest	String	Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is `now`.
metric_name	String	**Required.** The name of a metric.

Returned values

There are no returned values other than the dimension names.

Example request and response

XML Request

```
curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/dimensions?metric_name=*
```

XML Response

```
...
  <title>metricstore-dimensions</title>
  <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/dimensions</id>
  <updated>2017-12-19T00:02:27+00:00</updated>
  <generator build="31fcdba9ddc1" version="7.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/catalog/metricstore/dimensions/_acl" rel="_acl"/>
  <opensearch:totalResults>7</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>App</title>
    <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/dimensions/App</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/catalog/metricstore/dimensions/App" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/catalog/metricstore/dimensions/App" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">0</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>bbuser</s:item>
                    <s:item>cat_read</s:item>
                    <s:item>power</s:item>
                    <s:item>splunk-system-role</s:item>
                    <s:item>statsd</s:item>
                    <s:item>user</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

Another example request'

List all the dimension fields for the `os.mem.free` metric when the `dc` dimension field is limited to a value of `east`:

```
curl -k -u admin:passwd
https://localhost:8089/services/catalog/metricstore/dimensions?metric_name=os.mem.free&filter=dc%3deast
```

catalog/metricstore/dimensions/{dimension-name}/values

```
https://<host>:<mPort>/services/catalog/metricstore/dimensions/{dimension-name}/values
```

Use this endpoint to list values for a given `{dimension-name}`.

GET

Returns values of a `{dimension-name}` for a given metric.

Request parameters

Pagination and filtering parameters can be used with this method.

Name	Type	Description
earliest	String	Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is `-1d`.
filter	String	Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as index or dimension. For example, to specify a dimension named `os`, use `filter=os`. To specify two index names and values such as`index=index1` and `index=index2`, use `index%3dindex1%26index%3dindex2`.
latest	String	Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is `now`.
metric_name	String	**Required.** The name of a metric.

Returned values

There are no returned values other than those of the selected `{dimension-name}`.

Example request and response

XML Request

List all values for the `app` dimension of the `os.mem.free` metric:

```
curl -k -u statsd:statsd
https://localhost:8089/services/catalog/metricstore/dimensions/app/values?metric_name=os.mem.free
```

XML Response

```
...
  <title>metricstore-dimensions</title>
  <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/dimensions</id>
  <updated>2017-12-19T02:05:19+00:00</updated>
  <generator build="31fcdba9ddc1" version="7.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/catalog/metricstore/dimensions/_acl" rel="_acl"/>
  <opensearch:totalResults>7</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>accountmanagement</title>
    <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/dimensions
/accountmanagement</id>
    <updated>1970-01-01T00:00:00+00:00</updated>
    <link href="/services/catalog/metricstore/dimensions/accountmanagement" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/catalog/metricstore/dimensions/accountmanagement" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">0</s:key>
            <s:key name="can_write">0</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>bbuser</s:item>
                    <s:item>cat_read</s:item>
                    <s:item>power</s:item>
                    <s:item>splunk-system-role</s:item>
                    <s:item>statsd</s:item>
                    <s:item>user</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

More example requests

- List all values for the `dc` dimension of the `os.mem.free` metric, where `dc` is limited to a value of `east`:

```
curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/dimensions/dc/values?metric
_name=os.mem.free&filter=dc%3deast
```

- List all values for the `dc` dimension of the `mem.free` metric, where the recorded measurements also have an `os` dimension field:

```
curl -k -u admin:changeme  https://localhost:8089/services/catalog/metricstore/rollup
```

catalog/metricstore/rollup

```
https://<host>:<mPort>/services/catalog/metricstore/rollup
```

Use this endpoint to retrieve lists of metric indexes and their rollup summaries and to create new rollup policies for a given metric index.

Authentication and authorization

Use of the GET operation for this endpoint is restricted to roles that have the `list_metrics_catalog` capability. Use of the POST operation for this endpoint is restricted to roles that have the `edit_metrics_rollup` capability.

GET

Returns rollup summaries and the metric indexes with which they are associated.

Request parameters

None specific to this method. This method can use pagination and filtering parameters.

Returned values

Name	Description
name	The source index name. Rollup summaries are made up of aggregated metric data points that are derived from the metric data points in a source index.
summaries	A comma-separated list of the rollup summaries associated with the source metric index. Each summary configuration consists of a `span` and a `rollup_index`. The `span` is the interval by which the search head generates the aggregated rollup metric data points that make up the summary. The `rollup_index` is the target index for the rollup summary. The endpoint uses the following format when it lists summaries: `<span_1>|<rollup_index_1>,<span_2>|<rollup_index_2>...<span_n>|<rollup_index_n>`

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/catalog/metricstore/rollup
```

XML response

```
...
  <entry>
    <title>index_s</title>
    <id>https://127.0.0.1:8101/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aggregation.foo1">min#avg</s:key>
        <s:key name="aggregation.foo2">count#avg</s:key>
        <s:key name="defaultAggregation">avg#max</s:key>
        <s:key name="dimensionList">app,region</s:key>
        <s:key name="dimensionListType">included</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms"/>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="metricList">foo3,foo4</s:key>
        <s:key name="metricListType">excluded</s:key>
        <s:key name="minSpanAllowed">300</s:key>
        <s:key name="summaries">
          <s:dict>
            <s:key name="0">
              <s:dict>
                <s:key name="rollupIndex">index_d_1h</s:key>
                <s:key name="span">1h</s:key>
              </s:dict>
            </s:key>
            <s:key name="1">
              <s:dict>
                <s:key name="rollupIndex">index_d_1d</s:key>
                <s:key name="span">1d</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Creates rollup policies for a specified metric index.

Request parameters

<table>
<tr><th>Name</th><th>Type</th><th>Description</th></tr>
<tr><td><i>name</i></td><td>String</td><td><b>Required.</b> Specify the name of the source metric index. This is the index from which the aggregated metric data points in the rollup summaries will be derived.</td></tr>
<tr><td><i>summaries</i></td><td>String</td><td><b>Required.</b> Specify one or more rollup summaries, separated by commas. A rollup summary is a combination of a rollup period and a rollup metric index.

The rollup period is the <code>span</code>. This time range string is the interval on which the search head generates the aggregated rollup metric data points that make up the summary.

The rollup <code>span</code> is limited to the following values for minutes, hours, and days. Other time units are not allowed.
<table>
<tr><th>Time unit</th><th>Valid values</th></tr>
<tr><td><code>m</code> (minutes)</td><td>1,2,3,4,5,6,10,12,20,30,60</td></tr>
<tr><td><code>h</code> (hours)</td><td>1,2,3,4,6,8,12,24</td></tr>
<tr><td><code>d</code> (days)</td><td>1</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Name</th><th>Type</th><th>Description</th></tr>
<tr><td></td><td></td><td><table><tr><th>Time unit</th><th>Valid values</th></tr><tr><td></td><td></td></tr></table>The rollup index is the target index for the rollup summary.

The endpoint uses the following format when it lists summaries: <code>&lt;span_1&gt;|<rollup_index_1>,<span_2>|<rollup_index_2>...<span_n>|<rollup_index _n&gt;</code>. Defaults to <code>1hr|&lt;name&gt;</code>.</td></tr>
<tr><td><em>default_agg</em></td><td>String</td><td><strong>Optional</strong>. A list of aggregation functions, separated by <code>#</code> characters. Provides the set of aggregation functions that the rollup search uses when it aggregates the metric data points in the source metric index for a rollup summary. The <code>defaultAggregation</code> can be overruled for specific metrics by the <code>aggregation.<metric_name&gt;</code> setting. This setting supports the following functions: <code>avg</code>, <code>count</code>, <code>max</code>, <code>median</code>, <code>min</code>, <code>perc&lt;int&gt;</code>, and <code>sum</code>. Defaults to <code>avg</code>.</td></tr>
<tr><td><em>metric_list</em></td><td>String</td><td><strong>Optional</strong>. A comma-separated list of metric names. All of the listed metrics must appear in the source metric index identified by the <code>name</code> parameter. This list works in conjunction with the <code>metric_list_type</code> parameter to create a filter at the search head that allows certain metrics to be rolled up but not others. Defaults to empty string.</td></tr>
<tr><td><em>metric_list_type</em></td><td>[included | excluded]</td><td><strong>Optional</strong>. Works in conjunction with the <code>metric_list</code> parameter to create a filter at the search head that allows certain metrics to be rolled up to the rollup summaries but not others. Defaults to <code>excluded</code>.<ul><li>Use <code>included</code> to indicate that the search head should filter out all available metrics from the set of metrics being rolled up to the rollup summaries, except for the metrics listed in <code>metric_list</code> parameter.</li><li>Use <code>excluded</code> to indicate that the search head should roll up all available metrics to the rollup summaries except the metrics listed in <code>metric_list</code> parameter.</li></ul></td></tr>
<tr><td><em>dimension_list</em></td><td>String</td><td><strong>Optional</strong>. A comma-separated list of dimensions that appear in the source metric index identified by the <code>name</code> parameter. This list corresponds to the <code>dimension_list_type</code> parameter, which determines whether this set of dimensions is included or excluded from the aggregated rollup metrics that the search head generates for the rollup summary. Defaults to empty string.</td></tr>
<tr><td><em>dimension_list_type</em></td><td>[included | excluded]</td><td><strong>Optional</strong>. Identifies whether the dimensions specified in the <code>dimension_list</code> parameter are included or excluded from the rollup metrics that are generated by the rollup policies for the rollup summaries. Defaults to <code>excluded</code>.<ul><li>Use <code>included</code> to indicate that the rollup metrics produced by the rollup policy filter out all dimensions except the dimensions listed in the <code>dimension_list</code> parameter.</li><li>Use <code>excluded</code> to indicate that the rollup metrics produced by the rollup policy include all available dimensions except the dimensions in the <code>dimension_list</code> parameter.</li></ul></td></tr>
<tr><td><em>metric_overrides</em></td><td>String</td><td><strong>Optional</strong>. Provides a comma-separated list of exclusion rules for a set of rollup policies. Use this setting to override the default aggregation for one or more metrics. Each metric override pairs a metric name with one or more aggregation functions separated by <code>#</code> characters. Each metric override uses the following syntax: <code>&lt;metric_name>|<aggregation_function_1>#<aggregation_function_2>#…<aggregation_function_n</code>. Only the following aggregation functions are allowed: <code>avg</code>, <code>count</code>, <code>max</code>, <code>median</code>, <code>min</code>, <code>perc&lt;int&gt;</code>, and <code>sum</code>. Defaults to empty string.</td></tr>
</table>

Returned values

Name	Description
aggregation.<metric_name>	Overrides the default aggregation or set of aggregations for the specified `metric_name` and gives it a different aggregation or set of aggregations instead. Defined by the `metric_overrides` argument.
defaultAggregation	The default aggregation methods for the rollup policy, separated by `#` characters.
dimensionList	Comma-separated list of dimensions to be included or excluded from the aggregations, depending on the value of `dimensionListType`.
dimensionListType	Indicates whether the `dimensionList` should be `included` or `excluded` from the rollup policy.
metricList	

Name	Description
	Comma-separated list of metrics to be included or excluded from the set of metrics rolled up to the summaries, depending on the value of `dimensionListType`
metricListType	Indicates whether the `metricList` should be `included` or `excluded` from the rollup policy.
rollup.<summary number>.rollupIndex	The target rollup index for a specific summary. Summaries are identified by the `<summary number>`.
rollup.<summary number>.span	The rollup span for a specific summary. Summaries are identified by the `<summary number>`.

Example request and response

Place this stanza in `metric_rollups.conf`:

```
 [index:index_s]
 aggregation.foo1 = min#avg
 aggregation.foo2 = count#avg
 defaultAggregation = avg#max
 dimensionList = app,region
 dimensionListType = included
 metricList = foo3,foo4
 metricListType = excluded
 rollup.0.rollupIndex = index_d_1h
 rollup.0.span = 1h
 rollup.1.rollupIndex = index_d_1d
 rollup.1.span = 1d
```

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/catalog/metricstore/rollup  -d name=index_s -d
default_agg=avg#max -d dimension_list="app,region" -d dimension_list_type=included -d
metric_overrides="foo2|count#avg,foo1|min#avg" -d summaries="1h|index_d_1h,1d|index_d_1d" -d
metric_list="foo3,foo4" -d metric_list_type=excluded
```

XML response

```
...
  <entry>
    <title>index_s</title>
    <id>https://127.0.0.1:8101/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aggregation.foo1">min#avg</s:key>
        <s:key name="aggregation.foo2">count#avg</s:key>
        <s:key name="defaultAggregation">avg#max</s:key>
        <s:key name="dimensionList">app,region</s:key>
        <s:key name="dimensionListType">included</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms"/>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="metricList">foo3,foo4</s:key>
        <s:key name="metricListType">excluded</s:key>
        <s:key name="minSpanAllowed">300</s:key>
        <s:key name="summaries">
          <s:dict>
            <s:key name="0">
              <s:dict>
                <s:key name="rollupIndex">index_d_1h</s:key>
                <s:key name="span">1h</s:key>
              </s:dict>
            </s:key>
            <s:key name="1">
              <s:dict>
                <s:key name="rollupIndex">index_d_1d</s:key>
                <s:key name="span">1d</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

catalog/metricstore/rollup/{index}

`https://<host>:<mPort>/services/catalog/metricstore/rollup/{index}`

Use this endpoint to:

- Retrieve a list of the rollup summaries associated with a specific source `{index}`.
- Update a rollup policy for a specific specific source `{index}`.
- Delete a rollup policy for a specific specific source `{index}`.

Authentication and Authorization

Use of the GET operation for this endpoint is restricted to roles that have the `list_metrics_catalog` capability. Usage of the POST and DELETE operations for this endpoint are restricted to roles that have the `edit_metrics_rollup` capability.

GET

Returns a list of the rollup summaries associated with a specific source `{index}`.

Request parameters

None specific to this method. This method can use pagination and filtering parameters.

Returned values

Name	Description
summaries	A comma-separated list of the rollup summaries associated with the source metric `{index}`. Each summary configuration consists of a `span` and a `rollup_index`. The span is the interval by which the search head generates the aggregated rollup metric data points that make up the summary. The `rollup_index` is the target index for the rollup summary. The endpoint uses the following format when it lists summaries: `<span_1>|<rollup_index_1>,<span_2>|<rollup_index_2>...<span_n>|<rollup_index _n>`

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/catalog/metricstore/rollup/index_s
```

XML response

```
...
  <entry>
    <title>index_s</title>
    <id>https://localhost:8089/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aggregation.foo1"> min#avg </s:key>
        <s:key name="aggregation.foo2"> count#avg </s:key>
        <s:key name="defaultAggregation"> avg#max </s:key>
        <s:key name="dimensionList">app,region</s:key>
        <s:key name="dimensionListType">included</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms"/>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
```

```
              <s:list>
                <s:item>default_agg</s:item>
                <s:item>dimension_list</s:item>
                <s:item>dimension_list_type</s:item>
                <s:item>isProxyRequest</s:item>
                <s:item>metric_overrides</s:item>
                <s:item>noProxy</s:item>
                <s:item>summaries</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="metricList">foo3,foo4</s:key>
        <s:key name="metricListType">excluded</s:key>
        <s:key name="minSpanAllowed">300</s:key>
        <s:key name="summaries">
          <s:dict>
            <s:key name="0">
              <s:dict>
                <s:key name="rollupIndex">index_d_1h</s:key>
                <s:key name="span">1h</s:key>
              </s:dict>
            </s:key>
            <s:key name="1">
              <s:dict>
                <s:key name="rollupIndex">index_d_1d</s:key>
                <s:key name="span">1d</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Updates a rollup policy for a specific source `{index}`.

Request parameters

At least one argument is required.

Name	Type	Description
default_agg	String	**Optional**. A list of aggregation functions, separated by `#` characters. Provides the set of aggregation functions that the rollup search uses when it aggregates the metric data points in the source metric index for a rollup summary. The `defaultAggregation` can be overruled for specific metrics by the `aggregation.<metric_name>` setting. This setting supports the following functions: `avg`, `count`, `max`, `median`, `min`, `perc<int>`, and `sum`. Defaults to `avg`.
metric_list	String	**Optional**. A comma-separated list of metric names. All of the listed metrics must appear in the source metric index identified by the `name` parameter. This list works in conjunction with the `metric_list_type` parameter to create a filter at the search head that allows certain metrics to be rolled up but not others. Defaults to empty string.

<table>
<tr><th>Name</th><th>Type</th><th>Description</th></tr>
<tr><td><i>metric_list_type</i></td><td>[included | excluded]</td><td><b>Optional</b>. Works in conjunction with the <code>metric_list</code> parameter to create a filter at the search head that allows certain metrics to be rolled up to the rollup summaries but not others. Defaults to <code>excluded</code>.<ul><li>Use <code>included</code> to indicate that the search head should filter out all available metrics from the set of metrics being rolled up to the rollup summaries, except for the metrics listed in <code>metric_list</code> parameter.</li><li>Use <code>excluded</code> to indicate that the search head should roll up all available metrics to the rollup summaries except the metrics listed in <code>metric_list</code> parameter.</li></ul></td></tr>
<tr><td><i>dimension_list</i></td><td>string</td><td><b>Optional.</b> A comma-separated list of dimensions that appear in the source index. This list corresponds to the <code>dimension_list_type</code> parameter, which determines whether this set of dimensions is included or excluded from the aggregated rollup metrics that the search head generates for the rollup summary. Defaults to empty string.</td></tr>
<tr><td><i>dimension_list_type</i></td><td>[included | excluded]</td><td><b>Optional</b>. Identifies whether the dimensions specified in the <code>dimension_list</code> parameter are included or excluded from the rollup metrics that are generated by the rollup policies for the rollup summaries.<ul><li>Use <code>included</code> to indicate that the rollup metrics produced by the rollup policy filter out all dimensions except the dimensions listed in the <code>dimension_list</code> parameter.</li><li>Use <code>excluded</code> to indicate that the rollup metrics produced by the rollup policy include all available dimensions except the dimensions in the <code>dimension_list</code> parameter.</li></ul></td></tr>
<tr><td><i>metric_overrides</i></td><td>String</td><td><b>Optional</b>. Provides a comma-separated list of exclusion rules for a set of rollup policies. Use this setting to override the default aggregation for one or more metrics. Each metric override pairs a metric name with one or more aggregation functions separated by <code>#</code> characters. Each metric override uses the following syntax: <code><metric_name>|<aggregation_function_1>#<aggregation_function_2>#…<aggregation_function_n</code>. Only the following aggregation functions are allowed: <code>avg</code>, <code>count</code>, <code>max</code>, <code>median</code>, <code>min</code>, <code>perc<int></code>, and <code>sum</code>. Defaults to empty string.</td></tr>
<tr><td><i>summaries</i></td><td>string</td><td><b>Optional</b>. Specify one or more rollup summaries, separated by commas. A rollup summary is a combination of a rollup period and a rollup metric index.<p>The rollup period is the <code>span</code>. It is the interval on which the search head generates the aggregated rollup metric data points that make up the summary.</p><p>The rollup <code>span</code> is limited to the following values for minutes, hours, and days. Other time units are not allowed.</p><table><tr><th>Time unit</th><th>Valid values</th></tr><tr><td><code>m</code> (minutes)</td><td>1,2,3,4,5,6,10,12,20,30,60</td></tr><tr><td><code>h</code> (hours)</td><td>1,2,3,4,6,8,12,24</td></tr><tr><td><code>d</code> (days)</td><td>1</td></tr></table><p>The rollup index is the target index for the rollup summary.</p><p>The endpoint uses the following format when it lists summaries: <code><span_1>|<rollup_index_1>,<span_2>|<rollup_index_2>...<span_n>|<rollup_index_n></code></p></td></tr>
</table>

Returned values

Name	Description
aggregation.<metric_name>	Overrides the default aggregation or set of aggregations for the specified `metric_name` and gives it a different aggregation or set of aggregations instead. Defined by the `metric_overrides` argument.
defaultAggregation	The default aggregation methods for the rollup policy, separated by `#` characters.

Name	Description
dimensionList	Comma-separated list of dimensions to be included or excluded from the aggregations, depending on the value of `dimensionListType`.
dimensionListType	Indicates whether the `dimensionList` should be `included` or `excluded` from the rollup policy.
metricList	Comma-separated list of metrics to be included or excluded from the set of metrics rolled up to the summaries, depending on the value of `dimensionListType`
metricListType	Indicates whether the `metricList` should be `included` or `excluded` from the rollup policy.
rollup.<summary number>.rollupIndex	The target rollup index for a specific summary. Summaries are identified by the `<summary number>`.
rollup.<summary number>.span	The rollup span for a specific summary. Summaries are identified by the `<summary number>`.

Example request and response

Place this stanza in `metric_rollups.conf`:

```
[index:index_s]
aggregation.foo1 = min#avg
aggregation.foo2 = count#avg
defaultAggregation = avg#max
dimensionList = app,region
dimensionListType = included
metricList = foo3,foo4
metricListType = excluded
numRollupPolicy = 1
rollup.0.rollupIndex = index_d_30m
rollup.0.span = 30m
```

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/catalog/metricstore/rollup/index_s -d
summaries="30m|index_d_30m"
```

XML response

```
...
  <entry>
    <title>index_s</title>
    <id>https://localhost:8089/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
    <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="aggregation.foo1">min#avg</s:key>
        <s:key name="aggregation.foo2">count#avg</s:key>
        <s:key name="defaultAggregation">avg#max</s:key>
        <s:key name="dimensionList">app,region</s:key>
        <s:key name="dimensionListType">included</s:key>
        <s:key name="eai:acl">
```

```
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms"/>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="metricList">foo3,foo4</s:key>
        <s:key name="metricListType">excluded</s:key>
        <s:key name="minSpanAllowed">300</s:key>
        <s:key name="summaries">
          <s:dict>
            <s:key name="0">
              <s:dict>
                <s:key name="rollupIndex">index_d_30m</s:key>
                <s:key name="span">30m</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

DELETE

Deletes a rollup policy for a specific source `{index}`.

Request parameters
None specific to this method.

Returned values
None specific to this method.

Example request and response

Remove the `[index:metric_x]` stanza from `metric_rollups.conf`.

XML Request

```
curl -k -u admin:changeme -X DELETE https://localhost:8089/services/catalog/metricstore/rollup/metric_x
```

XML response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metricstore_rollup</title>
  <id>https://localhost:8089/services/catalog/metricstore/rollup</id>
  <updated>2019-03-20T16:40:00-07:00</updated>
  <generator build="86a463dcd7353fbb093dddacb657f1314fff6529" version="20190319"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/catalog/metricstore/rollup/_new" rel="create"/>
  <link href="/services/catalog/metricstore/rollup/_reload" rel="_reload"/>
  <link href="/services/catalog/metricstore/rollup/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

Output endpoints

Output endpoint descriptions

Manage data from forwarders.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. Output endpoints are generally not accessible in Splunk Cloud Platform.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

data/outputs/tcp/default

`https://<host>:<mPort>/services/data/outputs/tcp/default`

Access to global `tcpout` properties.

GET

Returns the current `tcpout` properties.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
autoLB	Specifies whether Auto Load balance method is used.
defaultGroup	Target group names. The forwarder sends all data to the specified groups. Starting with 4.2, this attribute is no longer required.
disabled	Indicates if tcpout settings are disabled.
forwardedindex.0.whitelist	Specifies 0th whitelist filter. forwardedindex.<n>.whitelist decides which events get forwarded based on the indexes they belong to.
forwardedindex.1.blacklist	Specifies 1st blacklist filter. forwardedindex.<n>.blacklist specifies index for which events are not forwarded.
forwardedindex.2.whitelist	Specifies 2nd whitelist filter. forwardedindex.<n>.whitelist decides which events get forwarded based on the indexes they belong to.
forwardedindex.filter.disable	Specifies whether filtering of forwarded data based on index is diasbled.
indexAndForward	Specifies whether to index all data locally, in addition to forwarding it. Defaults to false. This is known as an "index-and-forward" configuration. This attribute is only available for heavy forwarders. It is available only at the top level [tcpout] stanza in outputs.conf. It cannot be overridden in a target group.
maxQueueSize	Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). See the parmeter description for the POST operation for more information.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default
```

XML Response

```
...
 <title>tcpout-default</title>
 <id>https://localhost:8089/services/data/outputs/tcp/default</id>
 <updated>2011-07-10T22:38:23-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
```

```
<link href="/services/data/outputs/tcp/default/_new" rel="create"/>
<link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>tcpout</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/default/tcpout</id>
  <updated>2011-07-10T22:38:23-07:00</updated>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="list"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="remove"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="autoLB">1</s:key>
      <s:key name="defaultGroup">spacecake_9998</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl nodes elided ...
      <s:key name="forwardedindex.0.whitelist">.*</s:key>
      <s:key name="forwardedindex.1.blacklist">_.*</s:key>
      <s:key name="forwardedindex.2.whitelist">_audit</s:key>
      <s:key name="forwardedindex.filter.disable">0</s:key>
      <s:key name="indexAndForward">0</s:key>
      <s:key name="maxQueueSize">500KB</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Configure global `tcpout` properties.

Request parameters

Name	Type	Default	Description
defaultGroup	String		Comma-separated list of one or more target group names, specified later in [tcpout:<target_group>] stanzas of outputs.conf.spec file. The forwarder sends all data to the specified groups. If you do not want to forward data automatically, do not set this attribute. Can be overridden by an inputs.conf _TCP_ROUTING setting, which in turn can be overridden by a props.conf/transforms.conf modifier. Starting with 4.2, this attribute is no longer required.
disabled	Boolean		Disables default tcpout settings
dropEventsOnQueueFull	Number		If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events).

Name	Type	Default	Description
			CAUTION: Do not set this value to a positive integer if you are monitoring files. Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group. Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.
heartbeatFrequency	Number		How often (in seconds) to send a heartbeat packet to the receiving server. Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.
indexAndForward	Boolean		Specifies whether to index all data locally, in addition to forwarding it. Defaults to false. This is known as an "index-and-forward" configuration. This attribute is only available for heavy forwarders. It is available only at the top level [tcpout] stanza in outputs.conf. It cannot be overridden in a target group.
maxQueueSize	Number		Specify an integer or integer[KB|MB|GB]. Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer. For heavy forwarders sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting. If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed data) or blocks of data (for unparsed data). A block of data is approximately 64KB. For non-parsing forwarders, such as universal forwarders, that send unparsed data, maxQueueSize is the maximum number of data blocks. If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).
name required	String		Configuration to be edited. The only valid value is "tcpout".
sendCookedData	Boolean		If true, events are cooked (processed by Splunk software). If false, events are raw and untouched prior to sending. Defaults to true.

Name	Type	Default	Description
			Set to false if you are sending to a third-party system.

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default/tcpout -d
'defaultGroup=myIndexers'
```

XML Response

```
...
 <title>tcpout-default</title>
 <id>https://localhost:8089/services/data/outputs/tcp/default</id>
 <updated>2011-07-10T22:43:53-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/default/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

data/outputs/tcp/default/{name}

`https://<host>:<mPort>/services/data/outputs/tcp/default/{name}`
Manage forwarder settings.

DELETE

Disable the default forwarding settings.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/data/outputs/tcp/default/tcpout
```

XML Response

```
...
<title>tcpout-default</title>
 <id>https://localhost:8085/services/data/outputs/tcp/default</id>
 <updated>2011-07-19T20:09:02-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/default/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

GET

Retrieve the named configuration.

Usage details
The only valid `{name}` here is "tcpout".

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default/tcpout
```

XML Response

```
...
<title>tcpout-default</title>
 <id>https://localhost:8089/services/data/outputs/tcp/default</id>
 <updated>2011-07-10T22:38:23-07:00</updated>
 <generator version="102807"/>
 <author>
```

```
    <name>Splunk</name>
  </author>
  <link href="/services/data/outputs/tcp/default/_new" rel="create"/>
  <link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>tcpout</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/default/tcpout</id>
    <updated>2011-07-10T22:38:23-07:00</updated>
    <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="list"/>
    <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="edit"/>
    <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="remove"/>
    <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="autoLB">1</s:key>
        <s:key name="defaultGroup">spacecake_9998</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl nodes elided ...
        <s:key name="forwardedindex.0.whitelist">.*</s:key>
        <s:key name="forwardedindex.1.blacklist">_.*</s:key>
        <s:key name="forwardedindex.2.whitelist">_audit</s:key>
        <s:key name="forwardedindex.filter.disable">0</s:key>
        <s:key name="indexAndForward">0</s:key>
        <s:key name="maxQueueSize">500KB</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Configure global forwarding properties.

Request parameters

Name	Type	Default	Description
defaultGroup	String		Comma-separated list of one or more target group names, specified later in [tcpout:<target_group>] stanzas of outputs.conf.spec file. The forwarder sends all data to the specified groups. If you do not want to forward data automatically, do not set this attribute. Can be overridden by an inputs.conf _TCP_ROUTING setting, which in turn can be overridden by a props.conf/transforms.conf modifier. Starting with 4.2, this attribute is no longer required.
disabled	Boolean		Disables default tcpout settings
dropEventsOnQueueFull	Number		If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events).

Name	Type	Default	Description
			Caution: Do not set this value to a positive integer if you are monitoring files. Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group. Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.
heartbeatFrequency	Number		How often (in seconds) to send a heartbeat packet to the receiving server. Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.
indexAndForward	Boolean		Specifies whether to index all data locally, in addition to forwarding it. Defaults to false. This is known as an "index-and-forward" configuration. This attribute is only available for heavy forwarders. It is available only at the top level [tcpout] stanza in outputs.conf. It cannot be overridden in a target group.
maxQueueSize	Number		Specify an integer or integer[KB|MB|GB]. Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer. For heavy forwarders sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting. If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed data) or blocks of data (for unparsed data). A block of data is approximately 64KB. For non-parsing forwarders, such as universal forwarders, that send unparsed data, maxQueueSize is the maximum number of data blocks. If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).
sendCookedData	Boolean		If true, events are cooked (processed by Splunk software). If false, events are raw and untouched prior to sending. Defaults to true. Set to false if you are sending to a third-party system.

Returned values

None

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default/tcpout -d
heartbeatFrequency=60
```

XML Response

```
...
 <title>tcpout-default</title>
 <id>https://localhost:8089/services/data/outputs/tcp/default</id>
 <updated>2011-07-10T22:43:53-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/default/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

data/outputs/tcp/group

`https://<host>:<mPort>/services/data/outputs/tcp/group`

Access to the configuration of a group of one or more data forwarding destinations.

Authentication and Authorization

- GET requires `list_forwarders` capability.
- POST requires `edit_forwarders` capability.

GET

Get configuration information about target groups.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
disabled	Indicates if tcpout is disabled for this group.

Name	Description
method	Specifies the type of output processor. Valid values: (tcpout | syslog)
servers	Servers included in this group.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group
```

XML Response

```
...
<title>tcpout-group</title>
 <id>https://localhost:8089/services/data/outputs/tcp/group</id>
 <updated>2011-07-10T22:21:07-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/group/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>spacecake_9998</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998</id>
   <updated>2011-07-10T22:21:07-07:00</updated>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998" rel="list"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">0</s:key>
       ... eai:acl nodes elided ...
       <s:key name="method">autobalance</s:key>
       <s:key name="servers">
         <s:list>
           <s:item>spacecake:9998</s:item>
         </s:list>
       </s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Configure a group of one or more data forwarding destinations.

Request parameters

Name	Type	Default	Description
compressed	Boolean	false	If true, forwarder sends compressed data. If set to true, the receiver port must also have compression turned on.
disabled	Boolean	false	If true, disables the group.
dropEventsOnQueueFull	Number	-1	If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events). **Caution:** Do not set this value to a positive integer if you are monitoring files. Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group. Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.
heartbeatFrequency	Number	30	How often (in seconds) to send a heartbeat packet to the group. Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.
maxQueueSize	Number	auto	Specify either an integer or integer[KB|MB|GB]. Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer. For heavy forwarders sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting. If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed data) or blocks of data (for unparsed data). A block of data is approximately 64KB. For non-parsing forwarders, such as universal forwarders, that send

Name	Type	Default	Description
			unparsed data, maxQueueSize is the maximum number of data blocks. If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).
method	Enum		Valid values: (tcpout | syslog) Specifies the type of output processor.
name required	String		The name of the group of receivers.
sendCookedData	Boolean	true	If true, send cooked events (events processed by Splunk software). If false, events are raw and untouched prior to sending. Set to false if you are sending to a third-party system. Defaults to true.
servers required	String		Comma-separated list of servers to include in the group.
token	GUID		Token value generated by the indexer after configuration.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group -d name=lan_receivers -d
method=autobalance -d servers=10.3.3.3:9997,10.4.4.4:9997
```

XML Response

```
...
 <title>tcpout-group</title>
 <id>https://localhost:8089/services/data/outputs/tcp/group</id>
 <updated>2011-07-10T22:21:23-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/group/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

data/outputs/tcp/group/{name}

```
https://<host>:<mPort>/services/data/outputs/tcp/group/{name}
```

Manage the `{name}` target group.

Authentication and Authorization

- GET requires `list_forwarders` capability.
- POST and DELETE require `edit_forwarders` capability.

DELETE

Deletes the target group specified by {name}.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE
https://localhost:8089/services/data/outputs/tcp/group/lan_receivers
```

XML Response

```
...
 <title>tcpout-group</title>
 <id>https://localhost:8089/services/data/outputs/tcp/group</id>
 <updated>2011-07-10T22:32:47-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/group/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

GET

Get configuration information about the target group specified by {name}.

Request parameters

None

Returned values

Name	Description
autoLB	Indicates if the forwarder performs automatic load balancing. See the description for the autoLB parameter in POST data/outputs/tcp/group for details.
disabled	Indicates if tcpout is disabled for this group.
method	Specifies the type of output processor. Valid values: (tcpout | syslog)
servers	Servers included in this group.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group/lan_receivers
```

XML Response

```
...
<title>tcpout-group</title>
 <id>https://localhost:8089/services/data/outputs/tcp/group</id>
 <updated>2011-07-10T22:23:10-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/group/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>lan_receivers</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers</id>
   <updated>2011-07-10T22:23:10-07:00</updated>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="list"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="remove"/>
   <content type="text/xml">
```

```
    <s:dict>
      <s:key name="autoLB">1</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl nodes elided ...
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>autoLB</s:item>
              <s:item>blockOnQueueFull</s:item>
              <s:item>compressed</s:item>
              <s:item>disabled</s:item>
              <s:item>dropEventsOnQueueFull</s:item>
              <s:item>heartbeatFrequency</s:item>
              <s:item>maxPersistentQueueSizeInMegs</s:item>
              <s:item>maxQueueSize</s:item>
              <s:item>method</s:item>
              <s:item>persistentQueuePath</s:item>
              <s:item>sendCookedData</s:item>
              <s:item>usePersistentQueue</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list>
              <s:item>servers</s:item>
            </s:list>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="method">autobalance</s:key>
      <s:key name="servers">
        <s:list>
          <s:item>10.3.3.3:9997</s:item>
          <s:item>10.4.4.4:9997</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update the configuration of the target group.

Request parameters

Name	Type	Default	Description
compressed	Boolean	false	If true, forwarder sends compressed data. If set to true, the receiver port must also have compression turned on.

Name	Type	Default	Description
disabled	Boolean	false	If true, disables the group.
dropEventsOnQueueFull	Number	-1	If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events). **Caution:** Do not set this value to a positive integer if you are monitoring files. Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group. Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.
heartbeatFrequency	Number	30	How often (in seconds) to send a heartbeat packet to the group. Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.
maxQueueSize	Number	auto	Specify either an integer or integer[KB|MB|GB]. Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer. For heavy forwarders sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting. If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed data) or blocks of data (for unparsed data). A block of data is approximately 64KB. For non-parsing forwarders, such as universal forwarders, that send unparsed data, maxQueueSize is the maximum number of data blocks. If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).
method	Enum		Valid values: (tcpout | syslog) Specifies the type of output processor.
sendCookedData	Boolean	true	If true, send cooked events (events processed by Splunk software).

Name	Type	Default	Description
			If false, events are raw and untouched prior to sending. Set to false if you are sending to a third-party system. Defaults to true.
servers required	String		Comma-separated list of servers to include in the group.
token	GUID		Token value generated by indexer after configuration.

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group/lan_receivers -d
maxQueueSize=1024KB -d servers=10.3.3.3:9997,10.4.4.4:9997
```

XML Response

```
...
 <title>tcpout-group</title>
 <id>https://localhost:8089/services/data/outputs/tcp/group</id>
 <updated>2011-07-10T22:26:02-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/group/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

data/outputs/tcp/server

```
https://<host>:<mPort>/services/data/outputs/tcp/server
```

Access data forwarding configurations.

GET

List existing forwarded servers.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
destHost	DNS name of the destination server.
destIp	IP address of the destination server.
destPort	Port on which the destination server is listening.
disabled	Indicates if the outputs to the destination server is disabled.
method	The data distribution method used when two or more servers exist in the same forwarder group. Valid values: (clone | balance | autobalance)
sourcePort	Port on destination server where data is forwarded.
status	Indicates the status of the connection to the server.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/server
```

XML Response

```
...
<title>tcpout-server</title>
 <id>https://localhost:8089/services/data/outputs/tcp/server</id>
 <updated>2011-07-10T21:34:59-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/server/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>spacecake:9998</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998</id>
   <updated>2011-07-10T21:34:59-07:00</updated>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998" rel="list"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/allconnections"
rel="allconnections"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/disable" rel="disable"/>
```

```
    <content type="text/xml">
      <s:dict>
        <s:key name="destHost">spacecake.splunk.com</s:key>
        <s:key name="destIp">10.1.1.73</s:key>
        <s:key name="destPort">9998</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl nodes elided ...
        <s:key name="method">autobalance</s:key>
        <s:key name="sourcePort">8085</s:key>
        <s:key name="status">connect_fail</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Creates a new forwarder output.

Request parameters

Name	Type	Default	Description
disabled	Boolean		If true, disables the forwarder.
method	Enum		Valid values: (clone | balance | autobalance) The data distribution method used when two or more servers exist in the same forwarder group.
name required	String		<host>:<port> of the Splunk receiver. <host> can be either an ip address or server name. <port> is the that port that the Splunk receiver is listening on.
sslAltNameToCheck	String		The alternate name to match in the remote server's SSL certificate.
sslCertPath	String		Path to the client certificate. If specified, connection uses SSL.
sslCipher	String		SSL Cipher in the form ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
sslCommonNameToCheck	String		Check the common name of the server's certificate against this name. If there is no match, assume that Splunk Enterprise is not authenticated against this server. You must specify this setting if sslVerifyServerCert is true.
sslPassword	String		The password associated with the CAcert. The default Splunk Enterprise CAcert uses the password "password."
sslRootCAPath	String		The path to the root certificate authority file (optional).
sslVerifyServerCert	Boolean		If true, make sure that the server you are connecting to is a valid one (authenticated). Both the common name and the alternate name of the server are then checked for a match.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/server -d name=tiny:9997
```

XML Response

```
  <title>tcpout-server</title>
 <id>https://localhost:8089/services/data/outputs/tcp/server</id>
 <updated>2011-07-10T21:35:13-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/server/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

data/outputs/tcp/server/{name}

`https://<host>:<mPort>/services/data/outputs/tcp/server/{name}`
Manage the `{name}` forwarder.

DELETE

Deletes the configuration for the `{name}` forwarded server.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/data/outputs/tcp/server/tiny:9997
```

XML Response

```
...
 <title>tcpout-server</title>
 <id>https://localhost:8089/services/data/outputs/tcp/server</id>
 <updated>2011-07-10T21:35:41-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/server/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

GET

Lists information for the `{name}` forwarded server.

Request parameters

None

Returned values

Name	Description
disabled	Indicates if the outputs to the destination server is disabled.
method	The data distribution method used when two or more servers exist in the same forwarder group. Valid values: (clone | balance | autobalance)

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/server/tiny:9997
```

XML Response

```
...
<title>tcpout-server</title>
 <id>https://localhost:8089/services/data/outputs/tcp/server</id>
 <updated>2011-07-10T21:35:24-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/server/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>tiny:9997</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997</id>
   <updated>2011-07-10T21:35:24-07:00</updated>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997" rel="list"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997" rel="remove"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997/allconnections"
rel="allconnections"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/server/tiny%3A9997/disable" rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">0</s:key>
       ... eai:acl nodes elided ...
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list>
               <s:item>backoffAtStartup</s:item>
               <s:item>disabled</s:item>
               <s:item>initialBackoff</s:item>
               <s:item>maxBackoff</s:item>
               <s:item>maxNumberOfRetriesAtHighestBackoff</s:item>
               <s:item>method</s:item>
               <s:item>sslAltNameToCheck</s:item>
               <s:item>sslCertPath</s:item>
               <s:item>sslCipher</s:item>
               <s:item>sslCommonNameToCheck</s:item>
               <s:item>sslPassword</s:item>
               <s:item>sslRootCAPath</s:item>
               <s:item>sslVerifyServerCert</s:item>
             </s:list>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="method">autobalance</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Configures the forwarded server specified by `{name}`.

Request parameters

Name	Type	Default	Description

disabled	Boolean		If true, disables the forwarder.
method	Enum		Valid values: (clone | balance | autobalance) The data distribution method used when two or more servers exist in the same forwarder group.
sslAltNameToCheck	String		The alternate name to match in the remote server's SSL certificate.
sslCertPath	String		Path to the client certificate. If specified, connection uses SSL.
sslCipher	String		SSL Cipher in the form ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
sslCommonNameToCheck	String		Check the common name of the server's certificate against this name. If there is no match, assume that Splunk Enterprise is not authenticated against this server. You must specify this setting if sslVerifyServerCert is true.
sslPassword	String		The password associated with the CAcert. The default Splunk Enterprise CAcert uses the password "password."
sslRootCAPath	String		The path to the root certificate authority file (optional).
sslVerifyServerCert	Boolean		If true, make sure that the server you are connecting to is a valid one (authenticated). Both the common name and the alternate name of the server are then checked for a match.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/server/tiny:9997 -d
initialBackoff=10
```

XML Response

```
...
 <title>tcpout-server</title>
 <id>https://localhost:8089/services/data/outputs/tcp/server</id>
 <updated>2011-07-10T21:35:33-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/server/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

data/outputs/tcp/server/{name}/allconnections

```
https://<host>:<mPort>/services/data/outputs/tcp/server/{name}/allconnections
```

Get `{name}` forwarder connections.

GET

List current connections to the `{name}` forwarded server.

Request parameters

None

Returned values

Name	Description
destHost	DNS name of the destination server.
destIp	IP address of the destination server.
destPort	Port on which the destination server is listening.
sourcePort	Port on destination server where data is forwarded.
status	Indicates the status of the connection to the server.

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/services/data/outputs/tcp/server/localhost%3A9997/allconnections
```

XML Response

```
...
<title>tcpout-server</title>
 <id>https://localhost:8089/services/data/outputs/tcp/server</id>
 <updated>2011-07-15T15:15:12-0700</updated>
 <generator version="101277"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/server/_new" rel="create"/>
 <link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>localhost:9997</title>
```

```
  <id>https://localhost:8089/services/data/outputs/tcp/server/localhost%3A9997</id>
  <updated>2011-07-15T15:15:12-0700</updated>
  <link href="/services/data/outputs/tcp/server/localhost%3A9997" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/outputs/tcp/server/localhost%3A9997" rel="list"/>
  <link href="/services/data/outputs/tcp/server/localhost%3A9997/_reload" rel="_reload"/>
  <link href="/services/data/outputs/tcp/server/localhost%3A9997" rel="edit"/>
  <link href="/services/data/outputs/tcp/server/localhost%3A9997" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="destHost">localhost</s:key>
      <s:key name="destIp">127.0.0.1</s:key>
      <s:key name="destPort">9997</s:key>
      ... eai:acl nodes elided ...
      <s:key name="sourcePort">8089</s:key>
      <s:key name="status">connect_done</s:key>
    </s:dict>
  </content>
</entry>
```

data/outputs/tcp/syslog

```
https://<host>:<mPort>/services/data/outputs/tcp/syslog
```

Access the configuration of a forwarded server configured to provide data in standard syslog format.

GET

Provides access to syslog data forwarding configurations.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
disabled	Specifies whether global syslog configuration is disabled.
server	Specifies server:port where data is forwarded.
type	Specifies whether tcp or udp is used to forward data. If unspecified, udp is used. Valid values : (tcp | udp).

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog
```

XML Response

```
...
<title>syslog</title>
 <id>https://localhost:8089/services/data/outputs/tcp/syslog</id>
 <updated>2011-07-21T22:16:11-0700</updated>
 <generator version="101277"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/syslog/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>myServers</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers</id>
   <updated>2011-07-21T22:16:11-0700</updated>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="list"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">1</s:key>
       ... eai:acl nodes elided ...
       <s:key name="server">syslogservers.splunk.com:514</s:key>
       <s:key name="type">tcp</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Configures a forwarder to send data in standard syslog format

Request parameters

Name	Type	Default	Description
disabled	Boolean		If true, disables global syslog settings.
name required	String		Name of the syslog output group. This is name used when creating syslog configuration in `outputs.conf`.
priority	Number		Sets syslog priority value. The priority value should specified as an integer. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.
server	String		host:port of the server where syslog data should be sent

Name	Type	Default	Description
syslogSourceType	String		Specifies a rule for handling data in addition to that provided by the "syslog" sourcetype. By default, there is no value for syslogSourceType. This string is used as a substring match against the sourcetype key. For example, if the string is set to 'syslog', then all source types containing the string "syslog" receives this special treatment. To match a source type explicitly, use the pattern "sourcetype::sourcetype_name." For example syslogSourcetype = sourcetype::apache_common Data that is "syslog" or matches this setting is assumed to already be in syslog format. Data that does not match the rules has a header, potentially a timestamp, and a hostname added to the front of the event. This is how Splunk software causes arbitrary log data to match syslog expectations.
timestampformat	String		Format of timestamp to add at start of the events to be forwarded. The format is a strftime-style timestamp formatting string. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.
type	String		Protocol to use to send syslog data. Valid values: (tcp | udp).

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog -d myServers -d
server=my.server.com:514
```

XML Response

```
...
<title>syslog</title>
 <id>https://localhost:22090/services/data/outputs/tcp/syslog</id>
 <updated>2011-07-21T23:00:26-07:00</updated>
 <generator version="104359"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/syslog/_new" rel="create"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

data/outputs/tcp/syslog/{name}

`https://<host>:<mPort>/services/data/outputs/tcp/syslog/{name}`
Manage configuration for the `{name}` forwarder.

DELETE

Deletes the configuration for the `{name}` forwarder.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/data/outputs/tcp/syslog/myServers
```

XML Response

```
...
 <title>syslog</title>
 <id>https://localhost:8089/services/data/outputs/tcp/syslog</id>
 <updated>2011-07-21T22:20:52-0700</updated>
 <generator version="101277"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/syslog/_new" rel="create"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

GET

Returns configuration information for the `{name}` forwarder.

Request parameters

None

Returned values

Name	Description
disabled	Specifies whether global syslog configuration is disabled.
server	Specifies server:port where data is forwarded.
type	Specifies whether tcp or udp is used to forward data. If unspecified, udp is used. Valid values : (tcp | udp).

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog/myServers
```

XML Response

```
...
<title>syslog</title>
 <id>https://localhost:8089/services/data/outputs/tcp/syslog</id>
 <updated>2011-07-21T22:30:33-0700</updated>
 <generator version="101277"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/syslog/_new" rel="create"/>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>myServers</title>
   <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers</id>
   <updated>2011-07-21T22:30:33-0700</updated>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="list"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="edit"/>
   <link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">1</s:key>
       ... eai:acl nodes elided ...
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list/>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
```

```
            <s:list/>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="server">syslogservers.splunk.com:514</s:key>
      <s:key name="type">tcp</s:key>
    </s:dict>
  </content>
</entry>
```

POST

Updates the configuration of the `{name}` forwarder.

Request parameters

Name	Type	Default	Description
disabled	Boolean		If true, disables global syslog settings.
priority	Number		Sets syslog priority value. The priority value should specified as an integer. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.
server	String		host:port of the server where syslog data should be sent
syslogSourceType	String		Specifies a rule for handling data in addition to that provided by the "syslog" sourcetype. By default, there is no value for syslogSourceType. This string is used as a substring match against the sourcetype key. For example, if the string is set to 'syslog', then all source types containing the string "syslog" receives this special treatment. To match a source type explicitly, use the pattern "sourcetype::sourcetype_name." For example syslogSourcetype = sourcetype::apache_common Data that is "syslog" or matches this setting is assumed to already be in syslog format. Data that does not match the rules has a header, potentially a timestamp, and a hostname added to the front of the event. This is how Splunk software causes arbitrary log data to match syslog expectations.
timestampformat	String		Format of timestamp to add at start of the events to be forwarded. The format is a strftime-style timestamp formatting string. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.
type	String		Protocol to use to send syslog data. Valid values: (tcp | udp).

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog/myServers -d type=udp
```

XML Response

```
...
 <title>syslog</title>
 <id>https://localhost:8089/services/data/outputs/tcp/syslog</id>
 <updated>2011-07-21T22:53:23-07:00</updated>
 <generator version="104359"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/data/outputs/tcp/syslog/_new" rel="create"/>
 <opensearch:totalResults>0</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
```

Search endpoints

Search endpoint descriptions

Manage search resources including alerts triggered by searches, Python search command information, saved searches, search results, and scheduled view objects.

Semantic API versioning

Beginning with Splunk Enterprise version 9.0.1 and Splunk Cloud Platform version 9.0.2208, some REST API endpoints are available in multiple versions. The v1 instances of some endpoints are deprecated, and v2 instances of these endpoints are available. Plan to migrate to the v2 instances of each of the following endpoints:

- search/v2/jobs/export
- search/v2/jobs/{search_id}/events
- search/v2/jobs/{search_id}/results
- search/v2/jobs/{search_id}/results_preview
- search/v2/parser

You can address all original v1 endpoints either without a version number or with a v1 in the URI, but you can address v2 endpoints only with a v2 in the URI. Refer to the individual v2 endpoints for examples.

Legacy versioning deprecation

Beginning with Splunk Enterprise 9.0.1, the legacy versioning scheme from Splunk Enterprise 6.1 and lower is deprecated and will be removed in future versions of Splunk Enterprise. REST API endpoint behavior will not vary by Splunk Enterprise product version, but rather by API version only.

Do not include a Splunk Enterprise version number in URIs. Plan to migrate to the semantic versioning scheme with only v1 or v2 specified in URIs.

Avoid versioning endpoints like the following example:

```
https://localhost:8089/v6.1/services/search/jobs/export
```

Instead, refer to this v1 endpoint without any version or with v1 only, like the following example:

```
https://localhost:8089/services/search/jobs/export

https://localhost:8089/services/search/v1/jobs/export
```

Refer to this v2 endpoint like the following example:

```
https://localhost:8089/services/search/v2/jobs/export
```

Locate the source of your deprecated REST calls

If any apps or users in your environment are still using deprecated REST API version 1.0 endpoints, you should identify the source of the calls and transition all apps and users to version 2 instances of those endpoints.

1. Identify which apps are making deprecated REST calls by running the following search, which lists the calls to each deprecated endpoint in use by any apps in your environment.

   ```
   index=_internal source=*splunkd*.log "A REST call to the deprecated endpoint"
   ```

   Once you have identified which apps are using the deprecated endpoints, update the apps to make sure that they call version 2 instances of those endpoints instead.
2. After you're sure that all apps in your environment have been upgraded to the version 2 REST API endpoints, check whether any users are still calling the deprecated endpoints. Run the following search, which lists the users and deprecated endpoints they are calling.

   ```
   index=_internal (sourcetype=splunkd_access) method="GET" | where uri like
   "%/results_preview?search=%" OR uri like "%/results_preview?%&search=%" OR uri like
   "%/events?search=%" OR uri like "%/events?%&search=%" OR uri like "%/results?search=%" OR uri like
   "%/results?%&search=%" OR uri like "%/jobs/export?search=%" OR uri like "%/jobs/export?%&search=%"
   OR uri like "%/jobs/export%" OR uri like "%/parser%" | table uri, user, useragent
   ```

   Now that you know which users are calling deprecated endpoints, let them know that they must upgrade to version 2 instances of those endpoints.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Use the following URL for Splunk Cloud deployments. If necessary, submit a support case using the Splunk Support Portal to open port 8089 on your deployment.

```
https://<deployment-name>.splunkcloud.com:8089
```

Free trial Splunk Cloud accounts cannot access the REST API.

See Using the REST API in Splunk Cloud in the the *Splunk REST API Tutorials* for more information.

alerts/alert_actions

```
https://<host>:<mPort>/services/alerts/alert_actions
```

Access alert actions.

GET

Access a list of alert actions.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Varies depending on the type of alert.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/-/alerts/alert_actions
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>alert_actions</title>
  <id>https://localhost:8089/servicesNS/-/-/alerts/alert_actions</id>
  <updated>2018-12-10T16:45:47-05:00</updated>
  <generator build="8c86330ac18" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/-/-/alerts/alert_actions/_reload" rel="_reload"/>
  <link href="/servicesNS/-/-/alerts/alert_actions/_acl" rel="_acl"/>
  <opensearch:totalResults>9</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>email</title>
    <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/email</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email" rel="list"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email" rel="edit"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="auth_password"></s:key>
        <s:key name="auth_username"></s:key>
        <s:key name="bcc"></s:key>
        <s:key name="cc"></s:key>
        <s:key
name="cipherSuite">ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE
-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128
-SHA256</s:key>
        <s:key name="command"><![CDATA[$action.email.preprocess_results{default=""}$ | sendemail
"results_link=$results.url$" "ssname=$name$" "graceful=$graceful{default=True}$"
"trigger_time=$trigger_time$" maxinputs="$action.email.maxresults{default=10000}$"
maxtime="$action.email.maxtime{default=5m}$" results_file="$results.file$"]]></s:key>
        <s:key name="content_type">html</s:key>
        <s:key name="description">Send an email notification to specified recipients</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">system</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="footer.text">If you believe you've received this email in error, please see your Splunk
administrator.

splunk > the engine for machine data</s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="format">table</s:key>
        <s:key name="from">splunk</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="icon_path">mod_alert_icon_email.png</s:key>
        <s:key name="include.results_link">1</s:key>
        <s:key name="include.search">0</s:key>
        <s:key name="include.trigger">0</s:key>
        <s:key name="include.trigger_time">0</s:key>
        <s:key name="include.view_link">1</s:key>
        <s:key name="inline">0</s:key>
        <s:key name="label">Send email</s:key>
        <s:key name="mailserver">localhost</s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="message.alert">The alert condition for '$name$' was triggered.</s:key>
        <s:key name="message.report">The scheduled report '$name$' has run.</s:key>
        <s:key name="pdf.footer_center">title</s:key>
        <s:key name="pdf.footer_enabled">1</s:key>
        <s:key name="pdf.footer_left">logo</s:key>
        <s:key name="pdf.footer_right">timestamp,pagination</s:key>
        <s:key name="pdf.header_center">description</s:key>
        <s:key name="pdf.header_enabled">1</s:key>
        <s:key name="pdf.html_image_rendering">1</s:key>
        <s:key name="pdfview"></s:key>
        <s:key name="preprocess_results"></s:key>
        <s:key name="priority">3</s:key>
        <s:key name="reportCIDFontList">gb cns jp kor</s:key>
        <s:key name="reportFileName">$name$-$time:%Y-%m-%d$</s:key>
        <s:key name="reportIncludeSplunkLogo">1</s:key>
        <s:key name="reportPaperOrientation">portrait</s:key>
        <s:key name="reportPaperSize">letter</s:key>
        <s:key name="sendcsv">0</s:key>
        <s:key name="sendpdf">0</s:key>
        <s:key name="sendresults">0</s:key>
        <s:key name="sslVersions">tls1.2</s:key>
        <s:key name="subject">Splunk Alert: $name$</s:key>
        <s:key name="subject.alert">Splunk Alert: $name$</s:key>
        <s:key name="subject.report">Splunk Report: $name$</s:key>
        <s:key name="to"></s:key>
        <s:key name="track_alert">1</s:key>
        <s:key name="ttl">86400</s:key>
        <s:key name="useNSSubject">0</s:key>
        <s:key name="use_ssl">0</s:key>
        <s:key name="use_tls">0</s:key>
        <s:key name="width_sort_columns">1</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>logevent</title>
    <id>https://localhost:8089/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent" rel="list"/>
    <link href="/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent" rel="edit"/>
    <link href="/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="command">sendalert $action_name$ results_file="$results.file$"
results_link="$results.url$"</s:key>
        <s:key name="description">Send log event to Splunk receiver endpoint</s:key>
        <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">alert_logevent</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">global</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:appName">alert_logevent</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="forceCsvResults">auto</s:key>
      <s:key name="hostname"></s:key>
      <s:key name="icon_path">logevent.png</s:key>
      <s:key name="is_custom">1</s:key>
      <s:key name="label">Log Event</s:key>
      <s:key name="maxresults">10000</s:key>
      <s:key name="maxtime">5m</s:key>
      <s:key name="param.host"></s:key>
      <s:key name="param.index">main</s:key>
      <s:key name="param.source">alert:$name$</s:key>
      <s:key name="param.sourcetype">generic_single_line</s:key>
      <s:key name="payload_format">json</s:key>
      <s:key name="track_alert">0</s:key>
      <s:key name="ttl">10p</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>lookup</title>
  <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/lookup</id>
  <updated>1969-12-31T19:00:00-05:00</updated>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup" rel="list"/>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup" rel="edit"/>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
```

```
        <s:key name="append">0</s:key>
        <s:key name="command">outputlookup "$action.lookup.filename$" append=$action.lookup.append$</s:key>
        <s:key name="description">Output the results of the search to a CSV lookup file</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">system</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="filename"></s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="icon_path">mod_alert_icon_lookup.png</s:key>
        <s:key name="label">Output results to lookup</s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="track_alert">0</s:key>
        <s:key name="ttl">10p</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>outputtelemetry</title>
    <id>https://localhost:8089/servicesNS/nobody/splunk_instrumentation/alerts/alert_actions
/outputtelemetry</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/splunk_instrumentation/alerts/alert_actions/outputtelemetry"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/splunk_instrumentation/alerts/alert_actions/outputtelemetry" rel="list"/>
    <link href="/servicesNS/nobody/splunk_instrumentation/alerts/alert_actions/outputtelemetry/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/splunk_instrumentation/alerts/alert_actions/outputtelemetry" rel="edit"/>
    <link href="/servicesNS/nobody/splunk_instrumentation/alerts/alert_actions/outputtelemetry/disable"
```

```
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="command"><![CDATA[outputtelemetry input=$action.outputtelemetry.param.input$
anonymous=$action.outputtelemetry.param.anonymous$ license=$action.outputtelemetry.param.license$
support=$action.outputtelemetry.param.support$ component=$action.outputtelemetry.param.component$
type=$action.outputtelemetry.param.type$
optinrequired=$action.outputtelemetry.param.optinrequired$]]></s:key>
        <s:key name="description">Custom action to output results to telemetry endpoint</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">splunk_instrumentation</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">global</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">splunk_instrumentation</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="icon_path">outputtelemetry.png</s:key>
        <s:key name="is_custom">1</s:key>
        <s:key name="label">Output results to telemetry endpoint</s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="param.anonymous">1</s:key>
        <s:key name="param.component"></s:key>
        <s:key name="param.input"></s:key>
        <s:key name="param.license">0</s:key>
        <s:key name="param.optinrequired">1</s:key>
        <s:key name="param.support">1</s:key>
        <s:key name="param.type">event</s:key>
        <s:key name="track_alert">0</s:key>
        <s:key name="ttl">120</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>populate_lookup</title>
    <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/populate_lookup</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/populate_lookup" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/populate_lookup" rel="list"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/populate_lookup/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/populate_lookup" rel="edit"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/populate_lookup/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="command">copyresults dest="$action.populate_lookup.dest$"  sid="$search_id$"</s:key>
        <s:key name="dest"></s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">system</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="track_alert">0</s:key>
        <s:key name="ttl">120</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>rss</title>
    <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/rss</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/rss" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/rss" rel="list"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/rss/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/rss" rel="edit"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/rss/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="command">createrss "path=$name$.xml" "name=$name$" "link=$results.url$" "descr=Alert
trigger: $name$, results.count=$results.count$ " "count=30" "graceful=$graceful{default=1}$"
maxtime="$action.rss.maxtime{default=1m}$"</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">system</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">1m</s:key>
        <s:key name="track_alert">0</s:key>
        <s:key name="ttl">86400</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>script</title>
    <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/script</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/script" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/script" rel="list"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/script/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/script" rel="edit"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/script/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="command">runshellscript "$action.script.filename$" "$results.count$" "$search$"
"$search$" "$name$" "Saved Search [$name$] $counttype$($results.count$)" "$results.url$" "$deprecated_arg$"
"$search_id$" "$results.file$" maxtime="$action.script.maxtime{default=5m}$"</s:key>
        <s:key name="description">Invoke a custom script</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">system</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="filename"></s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="icon_path">mod_alert_icon_script.png</s:key>
        <s:key name="label">Run a script</s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="track_alert">1</s:key>
        <s:key name="ttl">600</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>summary_index</title>
    <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/summary_index</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/summary_index" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/summary_index" rel="list"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/summary_index/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/summary_index" rel="edit"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/summary_index/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_name">summary</s:key>
        <s:key name="command"><![CDATA[summaryindex spool=t uselb=t addtime=t
index="$action.summary_index._name{required=yes}$" file="$name_hash$_$#random$.stash_new" name="$name$"
marker="$action.summary_index*{format=$KEY=\\\"$VAL\\\",
key_regex="action.summary_index.(?!(?:command|inline|maxresults|maxtime|ttl|track_alert|(?:_.*))$)(.*)"}$"]]><
/s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">system</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="inline">1</s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="track_alert">0</s:key>
        <s:key name="ttl">120</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>webhook</title>
    <id>https://localhost:8089/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook" rel="list"/>
    <link href="/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook" rel="edit"/>
    <link href="/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="command">sendalert $action_name$ results_file="$results.file$"
results_link="$results.url$"</s:key>
        <s:key name="description">Generic HTTP POST to a specified URL</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">alert_webhook</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">global</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">alert_webhook</s:key>
        <s:key name="eai:userName">nobody</s:key>
        <s:key name="forceCsvResults">auto</s:key>
        <s:key name="hostname"></s:key>
        <s:key name="icon_path">webhook.png</s:key>
        <s:key name="is_custom">1</s:key>
        <s:key name="label">Webhook</s:key>
        <s:key name="maxresults">10000</s:key>
        <s:key name="maxtime">5m</s:key>
        <s:key name="param.user_agent">Splunk/$server.guid$</s:key>
        <s:key name="payload_format">json</s:key>
        <s:key name="track_alert">0</s:key>
        <s:key name="ttl">10p</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

alerts/fired_alerts

`https://<host>:<mPort>/services/alerts/fired_alerts`

Access fired alerts.

GET

Access a fired alerts summary.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
triggered_alert_count	Trigger count for this alert.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/-/alerts/fired_alerts
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>alerts</title>
  <id>https://localhost:8089/services/alerts/fired_alerts</id>
  <updated>2011-07-11T19:27:22-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  < opensearch nodes elided for brevity. >
  <s:messages/>
  <entry>
    <title>-</title>
    <id>https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts/-</id>
    <updated>2011-07-11T19:27:22-07:00</updated>
    <link href="/servicesNS/admin/search/alerts/fired_alerts/-" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/alerts/fired_alerts/-" rel="list"/>
    <content type="text/xml">
      <s:dict>
        < eai:acl elided >
        <s:key name="triggered_alert_count">0</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

alerts/fired_alerts/{name}

```
https://<host>:<mPort>/services/alerts/fired_alerts/{name}
```

Access or delete the `{name}` triggered alert.

GET

List unexpired triggered instances of this alert.

Request parameters

None

Returned values

Name	Description
actions	Any additional alert actions triggered by this alert.
alert_type	Indicates if the alert was historical or real-time.
digest_mode	
expiration_time_rendered	
savedsearch_name	Name of the saved search that triggered the alert.
severity	Indicates the severity level of an alert. Severity level ranges from Info, Low, Medium, High, and Critical. Default is Medium. Severity levels are informational in purpose and have no additional functionality.
sid	The search ID of the search that triggered the alert.
trigger_time	The time the alert was triggered.
trigger_time_rendered	
triggered_alerts	

Application usage

Specify - for {name} to return all fired alerts.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts/MyAlert
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>alerts</title>
  <id>https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts</id>
  <updated>2012-10-25T09:20:04-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <!-- opensearch nodes elided for brevity. -->
  <s:messages/>
  <entry>
    <title>rt_scheduler__admin__search__MyAlert_at_1351181001_5.31_1351181987</title>
    <id>https://localhost:8089/servicesNS/nobody/search/alerts/fired_alerts/rt_scheduler__admin__search_
_MyAlert_at_1351181001_5.31_1351181987</id>
    <updated>2012-10-25T09:19:47-07:00</updated>
    <link
href="/servicesNS/nobody/search/alerts/fired_alerts/rt_scheduler__admin__search__MyAlert_at_1351181001_5.31
_1351181987" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <published>2012-10-25T09:19:47-07:00</published>
    <link
href="/servicesNS/nobody/search/alerts/fired_alerts/rt_scheduler__admin__search__MyAlert_at_1351181001_5.31
_1351181987" rel="list"/>
    <link
href="/servicesNS/nobody/search/alerts/fired_alerts/rt_scheduler__admin__search__MyAlert_at_1351181001_5.31
_1351181987" rel="remove"/>
    <link
href="/servicesNS/nobody/search/search/jobs/rt_scheduler__admin__search__MyAlert_at_1351181001_5.31"
rel="job"/>
    <link href="/servicesNS/nobody/search/saved/searches/MyAlert" rel="savedsearch"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="actions"/>
        <s:key name="alert_type">real time</s:key>
        <s:key name="digest_mode">0</s:key>
        <!-- eai:acl elided -->
        <s:key name="expiration_time_rendered">2012-10-26 09:19:47 PDT</s:key>
        <s:key name="savedsearch_name">MyAlert</s:key>
        <s:key name="severity">3</s:key>
        <s:key name="sid">rt_scheduler__admin__search__MyAlert_at_1351181001_5.31</s:key>
        <s:key name="trigger_time">1351181987</s:key>
        <s:key name="trigger_time_rendered">2012-10-25 09:19:47 PDT</s:key>
        <s:key name="triggered_alerts">5</s:key>
      </s:dict>
    </content>
  </entry>
  . . . elided . . .
</feed>
```

DELETE

Delete the record of this triggered alert.

Request parameters

None.

Response keys

None.

Example request and response

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts/scheduler__admin__search_aGF2ZV9ldmVudHM_at
_1310437740_5d3dfde563194ffd_1310437749
```

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>alerts</title>
  <id>https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts</id>
  <updated>2011-07-11T19:35:25-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <!-- opensearch nodes elided for brevity. -->
  <s:messages/>
</feed>
```

alerts/metric_alerts

`https://<host>:<mPort>/services/alerts/metric_alerts`
This endpoint lets you access and create streaming metric alerts.

Authentication and authorization

Only users whose roles have the `metric_alerts` capability can use this endpoint.

GET

Access streaming metric alert configurations.

Request parameters

None specific to this method. Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
action.<action_name>	Indicates whether the `<action_name>` is enabled or disabled for a particular metric alert. Valid values for `action_name` are: • `email` • `logevent` • `rss` • `script` • `webhook` For more information about the alert action options see the `alert_actions.conf` file.

Name	Description
action.<action_name>.<parameter>	Overrides the setting defined for an action in the `alert_actions.conf` file with a new setting that is valid only for the metric alert configuration to which it is applied.
condition	Specifies an alert condition for one or more metric_name and aggregation pairs. The alert conditions can include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one `'<mstats_aggregation>(<metric_name>)'` clause in single quotes. The condition can also reference dimensions specified in the `groupby` setting.
description	Description of the metric alert.
filter	Provides one or more Boolean expressions like `<dimension_field>=<value>` to define the search result dataset to monitor for the alert condition. Does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'. Combines with the `metric_indexes` setting to provide the complete search filter for the alert.
groupby	The list of dimension fields, delimited by comma, for the group-by clause of the alert search. This leads to multiple aggregation values, one per group, instead of one single value.
label.<label-name>	Arbitrary key-value pairs for labeling this alert.
metric_indexes	Specifies one or more metric indexes, delimited by comma. Combines with the `filter` setting to provide the complete search filter for the alert.
splunk_ui.<label-name>	An arbitrary key-value pair that is automatically generated by the Splunk software for its internal use only. Do not change it.
trigger.expires	Sets the period of time that a triggered alert record displays on the Triggered Alerts page.
trigger.max_tracked	Specifies the maximum number of instances of this alert that can display in the Triggered Alerts page. When this threshold is passed, the Splunk software removes the earliest instances from the Triggered Alerts page to honor this maximum number.
trigger.suppress	Specifies the suppression period to silence alert actions and notifications. • The suppression period goes into effect when an alert is triggered. • During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out. • When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again.

Example request and response

XML Request

```
$ curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T15:03:59-07:00</updated>
```

```
<generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/alerts/metric_alerts/_new" rel="create"/>
<link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
<link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>malert-001</title>
  <id>https://localhost:8089/servicesNS/admin/search/alerts/metric_alerts/malert-001</id>
  <updated>2019-09-16T14:50:17-07:00</updated>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="list"/>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="edit"/>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="remove"/>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="_group_key">streamalert_0a01bceb2f9624ac</s:key>
      <s:key name="condition">'sum(spl.intr.resource_usage.Hostwide.data.cpu_count)'>=10</s:key>
      <s:key name="description"></s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms"/>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">user</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:userName">admin</s:key>
      <s:key name="filter">region=east</s:key>
      <s:key name="groupby"></s:key>
      <s:key name="metric_indexes">_metrics</s:key>
      <s:key name="trigger.expires">24h</s:key>
      <s:key name="trigger.max_tracked">20</s:key>
      <s:key name="trigger.suppress"></s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>mpool used high</title>
  <id>https://localhost:8089/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high</id>
  <updated>2019-09-16T09:59:35-07:00</updated>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high" rel="alternate"/>
```

```
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high" rel="list"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high" rel="edit"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high" rel="remove"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_group_key">streamalert_d8b75eedcf404743</s:key>
        <s:key name="action.email">0</s:key>
        <s:key name="action.logevent">0</s:key>
        <s:key name="action.rss">0</s:key>
        <s:key name="action.script">0</s:key>
        <s:key name="action.webhook">1</s:key>
        <s:key name="action.webhook.command">sendalert $action_name$ results_file="$results.file$"
results_link="$results.url$"</s:key>
        <s:key name="action.webhook.description">Generic HTTP POST to a specified URL</s:key>
        <s:key name="action.webhook.forceCsvResults">auto</s:key>
        <s:key name="action.webhook.icon_path">webhook.png</s:key>
        <s:key name="action.webhook.is_custom">1</s:key>
        <s:key name="action.webhook.label">Webhook</s:key>
        <s:key name="action.webhook.maxresults">10000</s:key>
        <s:key name="action.webhook.maxtime">5m</s:key>
        <s:key name="action.webhook.param.user_agent">Splunk/$server.guid$</s:key>
        <s:key name="action.webhook.payload_format">json</s:key>
        <s:key name="action.webhook.track_alert">0</s:key>
        <s:key name="action.webhook.ttl">10p</s:key>
        <s:key name="condition">'max(spl.mlog.mpool.used)' > 10000</s:key>
        <s:key name="description">spl.mlog.mpool.used too high</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="filter"></s:key>
        <s:key name="groupby"></s:key>
        <s:key name="metric_indexes">_metrics</s:key>
        <s:key name="splunk_ui.displayview">analytics_workspace</s:key>
        <s:key name="splunk_ui.managedBy">Analytics Workspace</s:key>
        <s:key name="splunk_ui.severity">1</s:key>
        <s:key name="splunk_ui.track">1</s:key>
        <s:key name="trigger.expires">24h</s:key>
        <s:key name="trigger.max_tracked">20</s:key>
        <s:key name="trigger.suppress">3m</s:key>
        <s:key name="triggered_alert_count">20</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a streaming metric alert.

Request parameters

Name	Type	Description
action.<action-name>	Boolean	Indicates whether the `<action_name>` is enabled or disabled for a particular metric alert. Valid values for `action_name` are: • `email` • `logevent` • `rss` • `script` • `webhook` For more information about the alert action options see the `alert_actions.conf` file.
action.<action-name>.<parameter>	String	Override the global setting defined for an `<action-name>` in the `alert_actions.conf` file with a new setting that is valid only for the metric alert configuration to which it is applied.
condition required	Boolean `eval` expression	Specifies an alert condition for one or more metric_name and aggregation pairs. You can set alert conditions that include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one `'<mstats_aggregation>(<metric_name>)'` clause in single quotes. The condition can also reference dimensions specified in the `groupby` setting.
description	String	Provide a description of the streaming metric alert.
filter	String	Specify one or more Boolean expressions like `<dimension_field>=<value>` to define the search result dataset to monitor for an alert condition. Link multiple Boolean expressions with the `AND` operator. The filter does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'. This setting combines with the `metric_indexes` setting to provide the complete search filter for the alert.
groupby	String	Provide a list of dimension fields, delimited by comma, for the group-by clause of the alert search. This results in multiple aggregation values, one per group, instead of one aggregation value.
label.<label-name>	String	Provide an arbitrary key-value pair to label or tag this alert. This key-value pair is not used by the Splunk alerting framework. You can design applications that use the alert label when they call the \`alerts/metric_alerts\` endpoint.
metric_indexes required	String	Specify one or more metric indexes, delimited by comma. Combines with the filter setting to define the search result dataset that the alert monitors for the alert condition.
name required	String	Specify the name of the streaming metric alert.

Name	Type	Description
trigger.expires	String	Set the period of time that a triggered alert record displays on the Triggered Alerts page. • Use `<positive integer><time-unit>`, where `<time_unit>` can be 'm' for minutes, 'h' for hours, and 'd' for days. • Set to 0 to make triggered alerts expire immediately so they do not appear on the Triggered Alerts page at all. Default is 24h.
trigger.max_tracked	Number	Specify the maximum number of instances of this alert that can display in the triggered alerts dashboard. When this threshold is passed, the Splunk software removes the earliest jinstances from the dashboard to honor this maximum number. Set to 0 to remove the cap. Defaults to 20.
trigger.suppress	String	Define the suppression period to silence alert actions and notifications. • The suppression period goes into effect when an alert is triggered. • During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out. • When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again. Use `<number>`m to specify a timespan in minutes. Default is 0m.

Returned values

None.

Example request and response

XML Request

```
$ curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts -X POST -d name=malert-001
-d condition="'sum(spl.intr.resource_usage.Hostwide.data.cpu_count)'%3E%3D10" -d filter=region%3Deast -d
metric_indexes=_metrics
```

XML response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T15:07:52-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/alerts/metric_alerts/_new" rel="create"/>
  <link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
  <link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

```
</feed>
```

alerts/metric_alerts/{alert_name}

`https://<host>:<mPort>/services/alerts/metric_alerts/{alert_name}`
This endpoint lets you create, update, delete, enable, and disable streaming metric alerts.

Authentication and authorization

Only users whose roles have the `metric_alerts` capability can use this endpoint.

GET

Access the named streaming metric alert.

Request parameters

None specific to this method. Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
action.<action_name>	Indicates whether the `<action_name>` is enabled or disabled for a particular metric alert. Valid values for `action_name` are: • `email` • `logevent` • `rss` • `script` • `webhook` For more information about the alert action options see the `alert_actions.conf` file.
action.<action_name>.<parameter>	Overrides the setting defined for an action in the `alert_actions.conf` file with a new setting that is valid only for the metric alert configuration to which it is applied.
condition	Specifies an alert condition for one or more metric_name and aggregation pairs. The alert conditions can include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one `'<mstats_aggregation>(<metric_name>)'` clause in single quotes. The condition can also reference dimensions specified in the `groupby` setting.
description	Description of the metric alert.
groupby	The list of dimension fields, delimited by comma, for the group-by clause of the alert search. This leads to multiple aggregation values, one per group, instead of one single value.
filter	Provides one or more Boolean expressions like `<dimension_field>=<value>` to define the search result dataset to monitor for the alert condition. Does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'. Combines with the `metric_indexes` setting to provide the complete search filter for the alert.
label.<label-name>	Arbitrary key-value pairs for labeling this alert.
metric_indexes	

Name	Description
	Specifies one or more metric indexes, delimited by comma. Combines with the `filter` setting to provide the complete search filter for the alert.
splunk_ui.<label-name>	An arbitrary key-value pair that is automatically generated by the Splunk software for its internal use only. Do not change it.
trigger.expires	Sets the period of time that a triggered alert record displays on the Triggered Alerts page.
trigger.max_tracked	Specifies the maximum number of instances of this alert that can display in the Triggered Alerts page. When this threshold is passed, the Splunk software removes the earliest instances from the Triggered Alerts page to honor this maximum number.
trigger.suppress	Specifies the suppression period to silence alert actions and notifications. • The suppression period goes into effect when an alert is triggered. • During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out. • When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again.

Example request and response

XML Request

```
$ curl -k -u admin:pass123 https://localhost:8089/services/alerts/metric_alerts/malert-001
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T14:51:17-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/alerts/metric_alerts/_new" rel="create"/>
  <link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
  <link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>malert-001</title>
    <id>https://localhost:8089/servicesNS/admin/search/alerts/metric_alerts/malert-001</id>
    <updated>2019-09-16T14:50:17-07:00</updated>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="list"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="edit"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="remove"/>
    <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_group_key">streamalert_0a01bceb2f9624ac</s:key>
        <s:key name="action.email">0</s:key>
        <s:key name="action.email.auth_password"></s:key>
        <s:key name="action.email.auth_username"></s:key>
        <s:key name="action.email.bcc"></s:key>
        <s:key name="action.email.cc"></s:key>
        <s:key
name="action.email.cipherSuite">ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM
-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128
-SHA256:ECDHE-RSA-AES128-SHA256</s:key>
        <s:key name="action.email.command"><![CDATA[$action.email.preprocess_results{default=""}$ |
sendemail "results_link=$results.url$" "ssname=$name$" "graceful=$graceful{default=True}$"
"trigger_time=$trigger_time$" maxinputs="$action.email.maxresults{default=10000}$"
maxtime="$action.email.maxtime{default=5m}$" results_file="$results.file$"]]></s:key>
        <s:key name="action.email.content_type">html</s:key>
        <s:key name="action.email.description">Send an email notification to specified recipients</s:key>
        <s:key name="action.email.footer.text">If you believe you've received this email in error, please
see your Splunk administrator.

splunk > the engine for machine data</s:key>
        <s:key name="action.email.forceCsvResults">auto</s:key>
        <s:key name="action.email.format">table</s:key>
        <s:key name="action.email.from">splunk</s:key>
        <s:key name="action.email.hostname"></s:key>
        <s:key name="action.email.icon_path">mod_alert_icon_email.png</s:key>
        <s:key name="action.email.include.results_link">1</s:key>
        <s:key name="action.email.include.search">0</s:key>
        <s:key name="action.email.include.trigger">0</s:key>
        <s:key name="action.email.include.trigger_time">0</s:key>
        <s:key name="action.email.include.view_link">1</s:key>
        <s:key name="action.email.inline">0</s:key>
        <s:key name="action.email.label">Send email</s:key>
        <s:key name="action.email.mailserver">localhost</s:key>
        <s:key name="action.email.maxresults">10000</s:key>
        <s:key name="action.email.maxtime">5m</s:key>
        <s:key name="action.email.message.alert">The alert condition for '$name$' was triggered.</s:key>
        <s:key name="action.email.message.report">The scheduled report '$name$' has run.</s:key>
        <s:key name="action.email.pdf.footer_center">title</s:key>
        <s:key name="action.email.pdf.footer_enabled">1</s:key>
        <s:key name="action.email.pdf.footer_left">logo</s:key>
        <s:key name="action.email.pdf.footer_right">timestamp,pagination</s:key>
        <s:key name="action.email.pdf.header_center">description</s:key>
        <s:key name="action.email.pdf.header_enabled">1</s:key>
        <s:key name="action.email.pdf.html_image_rendering">1</s:key>
        <s:key name="action.email.pdfview"></s:key>
        <s:key name="action.email.preprocess_results"></s:key>
        <s:key name="action.email.priority">3</s:key>
        <s:key name="action.email.reportCIDFontList">gb cns jp kor</s:key>
        <s:key name="action.email.reportFileName">$name$-$time:%Y-%m-%d$</s:key>
        <s:key name="action.email.reportIncludeSplunkLogo">1</s:key>
        <s:key name="action.email.reportPaperOrientation">portrait</s:key>
        <s:key name="action.email.reportPaperSize">letter</s:key>
        <s:key name="action.email.sendcsv">0</s:key>
        <s:key name="action.email.sendpdf">0</s:key>
        <s:key name="action.email.sendresults">0</s:key>
        <s:key name="action.email.sslVersions">tls1.2</s:key>
        <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
        <s:key name="action.email.subject.alert">Splunk Alert: $name$</s:key>
        <s:key name="action.email.subject.report">Splunk Report: $name$</s:key>
        <s:key name="action.email.to"></s:key>
        <s:key name="action.email.track_alert">1</s:key>
        <s:key name="action.email.ttl">86400</s:key>
        <s:key name="action.email.useNSSubject">0</s:key>
        <s:key name="action.email.use_ssl">0</s:key>
        <s:key name="action.email.use_tls">0</s:key>
        <s:key name="action.email.width_sort_columns">1</s:key>
        <s:key name="action.logevent">0</s:key>
        <s:key name="action.logevent.command">sendalert $action_name$ results_file="$results.file$"
results_link="$results.url$"</s:key>
        <s:key name="action.logevent.description">Send log event to Splunk receiver endpoint</s:key>
        <s:key name="action.logevent.forceCsvResults">auto</s:key>
        <s:key name="action.logevent.hostname"></s:key>
        <s:key name="action.logevent.icon_path">logevent.png</s:key>
        <s:key name="action.logevent.is_custom">1</s:key>
        <s:key name="action.logevent.label">Log Event</s:key>
        <s:key name="action.logevent.maxresults">10000</s:key>
        <s:key name="action.logevent.maxtime">5m</s:key>
        <s:key name="action.logevent.param.host"></s:key>
        <s:key name="action.logevent.param.index">main</s:key>
        <s:key name="action.logevent.param.source">alert:$name$</s:key>
        <s:key name="action.logevent.param.sourcetype">generic_single_line</s:key>
        <s:key name="action.logevent.payload_format">json</s:key>
        <s:key name="action.logevent.track_alert">0</s:key>
        <s:key name="action.logevent.ttl">10p</s:key>
        <s:key name="action.lookup">0</s:key>
        <s:key name="action.lookup.append">0</s:key>
        <s:key name="action.lookup.command">outputlookup "$action.lookup.filename$"
append=$action.lookup.append$</s:key>
        <s:key name="action.lookup.description">Output the results of the search to a CSV lookup
file</s:key>
        <s:key name="action.lookup.filename"></s:key>
        <s:key name="action.lookup.forceCsvResults">auto</s:key>
        <s:key name="action.lookup.hostname"></s:key>
        <s:key name="action.lookup.icon_path">mod_alert_icon_lookup.png</s:key>
        <s:key name="action.lookup.label">Output results to lookup</s:key>
        <s:key name="action.lookup.maxresults">10000</s:key>
        <s:key name="action.lookup.maxtime">5m</s:key>
        <s:key name="action.lookup.track_alert">0</s:key>
        <s:key name="action.lookup.ttl">10p</s:key>
        <s:key name="action.populate_lookup">0</s:key>
        <s:key name="action.populate_lookup.command">copyresults dest="$action.populate_lookup.dest$"
 sid="$search_id$"</s:key>
        <s:key name="action.populate_lookup.dest"></s:key>
        <s:key name="action.populate_lookup.forceCsvResults">auto</s:key>
        <s:key name="action.populate_lookup.hostname"></s:key>
        <s:key name="action.populate_lookup.maxresults">10000</s:key>
        <s:key name="action.populate_lookup.maxtime">5m</s:key>
        <s:key name="action.populate_lookup.track_alert">0</s:key>
        <s:key name="action.populate_lookup.ttl">120</s:key>
        <s:key name="action.rss">0</s:key>
        <s:key name="action.rss.command">createrss "path=$name$.xml" "name=$name$" "link=$results.url$"
"descr=Alert trigger: $name$, results.count=$results.count$ " "count=30" "graceful=$graceful{default=1}$"
maxtime="$action.rss.maxtime{default=1m}$"</s:key>
        <s:key name="action.rss.forceCsvResults">auto</s:key>
        <s:key name="action.rss.hostname"></s:key>
        <s:key name="action.rss.maxresults">10000</s:key>
        <s:key name="action.rss.maxtime">1m</s:key>
        <s:key name="action.rss.track_alert">0</s:key>
        <s:key name="action.rss.ttl">86400</s:key>
        <s:key name="action.script">0</s:key>
        <s:key name="action.script.command">runshellscript "$action.script.filename$" "$results.count$"
```

```
"$search$" "$search$" "$name$" "Saved Search [$name$] $counttype$($results.count$)" "$results.url$"
"$deprecated_arg$" "$search_id$" "$results.file$" maxtime="$action.script.maxtime{default=5m}$"</s:key>
        <s:key name="action.script.description">Invoke a custom script</s:key>
        <s:key name="action.script.filename"></s:key>
        <s:key name="action.script.forceCsvResults">auto</s:key>
        <s:key name="action.script.hostname"></s:key>
        <s:key name="action.script.icon_path">mod_alert_icon_script.png</s:key>
        <s:key name="action.script.label">Run a script</s:key>
        <s:key name="action.script.maxresults">10000</s:key>
        <s:key name="action.script.maxtime">5m</s:key>
        <s:key name="action.script.track_alert">1</s:key>
        <s:key name="action.script.ttl">600</s:key>
        <s:key name="action.summary_index">0</s:key>
        <s:key name="action.summary_index._name">summary</s:key>
        <s:key name="action.summary_index.command"><![CDATA[summaryindex spool=t uselb=t addtime=t
index="$action.summary_index._name{required=yes}$" file="$name_hash$_$#random$.stash_new" name="$name$"
marker="$action.summary_index*{format=$KEY=\\\"$VAL\\\",
key_regex="action.summary_index.(?!(?:command|forceCsvResults|inline|maxresults|maxtime|python\\.version|ttl|track
_alert|(?:_.*))$)(.*)"}$"]]></s:key>
        <s:key name="action.summary_index.forceCsvResults">auto</s:key>
        <s:key name="action.summary_index.hostname"></s:key>
        <s:key name="action.summary_index.inline">1</s:key>
        <s:key name="action.summary_index.maxresults">10000</s:key>
        <s:key name="action.summary_index.maxtime">5m</s:key>
        <s:key name="action.summary_index.track_alert">0</s:key>
        <s:key name="action.summary_index.ttl">120</s:key>
        <s:key name="action.webhook">0</s:key>
        <s:key name="action.webhook.command">sendalert $action_name$ results_file="$results.file$"
results_link="$results.url$"</s:key>
        <s:key name="action.webhook.description">Generic HTTP POST to a specified URL</s:key>
        <s:key name="action.webhook.forceCsvResults">auto</s:key>
        <s:key name="action.webhook.hostname"></s:key>
        <s:key name="action.webhook.icon_path">webhook.png</s:key>
        <s:key name="action.webhook.is_custom">1</s:key>
        <s:key name="action.webhook.label">Webhook</s:key>
        <s:key name="action.webhook.maxresults">10000</s:key>
        <s:key name="action.webhook.maxtime">5m</s:key>
        <s:key name="action.webhook.param.user_agent">Splunk/$server.guid$</s:key>
        <s:key name="action.webhook.payload_format">json</s:key>
        <s:key name="action.webhook.track_alert">0</s:key>
        <s:key name="action.webhook.ttl">10p</s:key>
        <s:key name="condition">'sum(spl.intr.resource_usage.Hostwide.data.cpu_count)'>=10</s:key>
        <s:key name="description"></s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms"/>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">user</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
```

```
     <s:dict>
      <s:key name="optionalFields">
       <s:list>
        <s:item>condition</s:item>
        <s:item>description</s:item>
        <s:item>disabled</s:item>
        <s:item>filter</s:item>
        <s:item>groupby</s:item>
        <s:item>metric_indexes</s:item>
        <s:item>trigger.condition</s:item>
        <s:item>trigger.expires</s:item>
        <s:item>trigger.max_tracked</s:item>
        <s:item>trigger.per_group</s:item>
        <s:item>trigger.suppress</s:item>
       </s:list>
      </s:key>
      <s:key name="requiredFields">
       <s:list/>
      </s:key>
      <s:key name="wildcardFields">
       <s:list>
        <s:item>action\..*</s:item>
        <s:item>label\..*</s:item>
        <s:item>splunk_ui\..*</s:item>
       </s:list>
      </s:key>
     </s:dict>
    </s:key>
    <s:key name="eai:userName">admin</s:key>
    <s:key name="filter">region=east</s:key>
    <s:key name="groupby"></s:key>
    <s:key name="metric_indexes">_metrics</s:key>
    <s:key name="trigger.expires">24h</s:key>
    <s:key name="trigger.max_tracked">20</s:key>
    <s:key name="trigger.suppress"></s:key>
   </s:dict>
  </content>
 </entry>
</feed>
```

POST

Update the named streaming metric alert.

Request parameters

Name	Type	Description
action.<action-name>	Boolean	Indicates whether the `<action_name>` is enabled or disabled for a particular metric alert. Valid values for `<action_name>` are: • `email` • `logevent` • `rss` • `script` • `webhook` For more information about the alert action options see the `alert_actions.conf` file.
action.<action-name>.<parameter>	String	

Name	Type	Description
		Override the global setting defined for an `<action-name>` in the `alert_actions.conf` file with a new setting that is valid only for the metric alert configuration to which it is applied.
condition required	Boolean `eval` expression	Specifies an alert condition for one or more metric_name and aggregation pairs. You can set alert conditions that include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one `'<mstats_aggregation>(<metric_name>)'` clause in single quotes. The condition can also reference dimensions specified in the `groupby` setting.
description	String	Provide a description of the streaming metric alert.
groupby	String	Provide a list of dimension fields, delimited by comma, for the group-by clause of the alert search. This results in multiple aggregation values, one per group, instead of one aggregation value.
filter	String	Specify one or more Boolean expressions like `<dimension_field>=<value>` to define the search result dataset to monitor for an alert condition. Link multiple Boolean expressions with the 'AND' operator. The filter does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'. This setting combines with the `metric_indexes` setting to provide the complete search filter for the alert.
label.<label-name>	String	Provide an arbitrary key-value pair to label or tag this alert. This key-value pair is not used by the Splunk alerting framework. You can design applications that use the alert label when they call the `alerts/metric_alerts` endpoint.
metric_indexes required	String	Specify one or more metric indexes, delimited by comma. Combines with the filter setting to define the search result dataset that the alert monitors for the alert condition.
trigger.expires	String	Set the period of time that a triggered alert record displays on the Triggered Alerts page. • Use `<positive integer><time-unit>`, where `<time_unit>` can be 'm' for minutes, 'h' for hours, and 'd' for days. • Set to 0 to make triggered alerts expire immediately so they do not appear on the Triggered Alerts page at all. Default is 24h.
trigger.max_tracked	Number	Specify the maximum number of instances of this alert that can display in the triggered alerts dashboard. When this threshold is passed, the Splunk software removes the earliest instances from the dashboard to honor this maximum number. Set to 0 to remove the cap. Defaults to 20.
trigger.suppress	String	Define the suppression period to silence alert actions and notifications. • The suppression period goes into effect when an alert is triggered. • During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out. • When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again. Use `<number>`m to specify a timespan in minutes. Default is 0m.

Name	Type	Description

Returned values

None.

Example request and response

XML Request

```
$ curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts/malert-002 -d description="updated description of malert-002" -d trigger.expires=1h
```

XML response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T14:38:38-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/alerts/metric_alerts/_new" rel="create"/>
  <link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
  <link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

DELETE

Deletes the named metric alert.

Request parameters

None specific to this method.

Returned values

None specific to this method.

Example request and response

Remove the `[malert-002]` stanza from `metric_alerts.conf`.

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts/malert-002 -X DELETE
```

XML response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T14:38:38-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/alerts/metric_alerts/_new" rel="create"/>
  <link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
  <link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

data/commands

`https://<host>:<mPort>/services/data/commands`
Access Python search commands.

GET

Access Python search commands.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
changes_colorder	Indicates whether the script output should be used to change the column ordering of the fields.
disabled	Indicates if the command is disabled.
enableheader	Indicate whether or not your script is expecting header information or not. Currently, the only thing in the header information is an auth token. If set to true the command expects as input a head section + '\ ' then the csv input. *Note:* Should be set to true if you use splunk.Intersplunk
filename	Name of script file for command. <stanza-name>.pl for perl. <stanza-name>.py for python.
generates_timeorder	If generating = false and streaming = true, indicates if the command changes the order of events w/respect to time.
generating	Indicates if the command generates new events.
maxinputs	Maximum number of events that can be passed to the command for each invocation. This limit cannot exceed the value of maxresultrows in limits.conf.

Name	Description
	0 indicates no limit. Defaults to 50000.
outputheader	If true, the output of script should be a header section + blank line + csv output. If false, script output should be pure csv only.
passauth	If true, passes an authentication token on the start of input.
required_fields	A list of fields that this command may use. Informs previous commands that they should retain/extract these fields if possible. No error is generated if a field specified is missing. Defaults to '*'.
requires_preop	Indicates whether the command sequence specified by the streaming_preop key is required for proper execution or is it an optimization only. Default is false (stremaing_preop not required).
retainsevents	Indicates whether the command retains events (the way the sort/dedup/cluster commands do) or whether the command transforms them (the way the stats command does).
streaming	Indicates whether the command is streamable.
supports_getinfo	Indicates whether the command supports dynamic probing for settings (first argument invoked == __GETINFO__ or __EXECUTE__).
supports_rawargs	Indicates whether the command supports raw arguments being passed to it or if it uses parsed arguments (where quotes are stripped).
type	Specifies the type of command. The only valid value for this attribute is `python`.

Example request and response

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/commands
```

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>commandsconf</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/commands</id>
  <updated>2011-07-07T00:52:26-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/commands/_reload" rel="_reload"/>
  <s:messages/>
  <entry>
    <title>bucketdir</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/commands/bucketdir</id>
    <updated>2011-07-07T00:52:26-07:00</updated>
    <link href="/servicesNS/nobody/search/data/commands/bucketdir" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/commands/bucketdir" rel="list"/>
    <link href="/servicesNS/nobody/search/data/commands/bucketdir/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/commands/bucketdir/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="changes_colorder">1</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="enableheader">1</s:key>
        <s:key name="filename">bucketdir.py</s:key>
        <s:key name="generates_timeorder">0</s:key>
        <s:key name="generating">0</s:key>
        <s:key name="maxinputs">50000</s:key>
        <s:key name="outputheader">0</s:key>
        <s:key name="passauth">0</s:key>
        <s:key name="required_fields">*</s:key>
        <s:key name="requires_preop">0</s:key>
        <s:key name="retainsevents">0</s:key>
        <s:key name="streaming">0</s:key>
        <s:key name="supports_getinfo">0</s:key>
        <s:key name="supports_rawargs">1</s:key>
        <s:key name="type">python</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

data/commands/{name}

`https://<host>:<mPort>/services/data/commands/{name}`

Get information about the `{name}` python search command.

GET

Access search command information.

Request parameters

None

Returned values

Name	Description
changes_colorder	Indicates whether the script output should be used to change the column ordering of the fields.
disabled	Indicates if the command is disabled.
enableheader	Indicate whether or not your script is expecting header information or not. Currently, the only thing in the header information is an auth token. If set to true the command expects as input a head section + '\ ' then the csv input. *Note:* Should be set to true if you use splunk.Intersplunk
filename	Name of script file for command.

Name	Description
	<stanza-name>.pl for perl. <stanza-name>.py for python.
generates_timeorder	If generating = false and streaming = true, indicates if the command changes the order of events w/respect to time.
generating	Indicates if the command generates new events.
maxinputs	Maximum number of events that can be passed to the command for each invocation. This limit cannot exceed the value of maxresultrows in limits.conf. 0 indicates no limit. Defaults to 50000.
outputheader	If true, the output of script should be a header section + blank line + csv output. If false, script output should be pure csv only.
passauth	If true, passes an authentication token on the start of input.
required_fields	A list of fields that this command may use. Informs previous commands that they should retain/extract these fields if possible. No error is generated if a field specified is missing. Defaults to '*'.
requires_preop	Indicates whether the command sequence specified by the streaming_preop key is required for proper execution or is it an optimization only. Default is false (stremaing_preop not required).
retainsevents	Indicates whether the command retains events (the way the sort/dedup/cluster commands do) or whether the command transforms them (the way the stats command does).
streaming	Indicates whether the command is streamable.
supports_getinfo	Indicates whether the command supports dynamic probing for settings (first argument invoked == __GETINFO__ or __EXECUTE__).
supports_rawargs	Indicates whether the command supports raw arguments being passed to it or if it uses parsed arguments (where quotes are stripped).
type	Specifies the type of command. The only valid value for this attribute is `python`.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/commands/input
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>commandsconf</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/commands</id>
  <updated>2011-07-07T00:52:26-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/commands/_reload" rel="_reload"/>
  <s:messages/>
  <entry>
    <title>input</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/commands/input</id>
    <updated>2011-07-07T00:52:26-07:00</updated>
    <link href="/servicesNS/nobody/search/data/commands/input" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/commands/input" rel="list"/>
    <link href="/servicesNS/nobody/search/data/commands/input/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/commands/input/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="changes_colorder">1</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="enableheader">1</s:key>
        <s:key name="filename">input.py</s:key>
        <s:key name="generates_timeorder">0</s:key>
        <s:key name="generating">0</s:key>
        <s:key name="maxinputs">50000</s:key>
        <s:key name="outputheader">0</s:key>
        <s:key name="passauth">1</s:key>
        <s:key name="required_fields">*</s:key>
        <s:key name="requires_preop">0</s:key>
        <s:key name="retainsevents">0</s:key>
        <s:key name="streaming">0</s:key>
        <s:key name="supports_getinfo">0</s:key>
        <s:key name="supports_rawargs">1</s:key>
        <s:key name="type">python</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/searches

`https://<host>:<mPort>/services/saved/searches`
Access and create saved searches.

GET

Access saved search configurations.

Request parameters

Name	Type	Default	Description
earliest_time	String		For scheduled searches display all the scheduled times starting from this time (not just the next run time)
latest_time	String		For scheduled searches display all the scheduled times until this time (not just the next run time)
listDefaultActionArgs	Boolean		Indicates whether to list default actions.
add_orphan_field	Boolean		Indicates whether the response includes a boolean value for each saved search to show whether the search is orphaned, meaning that it has no valid owner. When *add_orphan_field* is set to `true`, the response includes the orphaned search indicators, either `0` to indicate that a search is not orphaned or `1` to indicate that the search is orphaned. Admins can use this setting to check for searches without valid owners and resolve related issues.

Pagination and filtering parameters can be used with this method.

This endpoint returns an unusually high number of values. To limit the number of returned values, specify the `f` filtering parameter.

Returned values

Name	Description
action.<action_name>	Indicates whether the `<action_name>` is enabled or disabled for a particular search. For more information about the alert action options see the `alert_actions.conf` file.
action.<action_name>.<parameter>	Overrides the setting defined for an action in the `alert_actions.conf` file with a new setting that is valid only for the search configuration to which it is applied.
action.email	Indicates the state of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart. Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.

Name	Description
action.email.format	Specify the format of text in the email. This value also applies to any attachments. Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates.
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. *Note:* This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct a url that can be referenced externally, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost." When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails. Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the global maximum number of search results to send when email.action is enabled.
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.reportServerEnabled	Not supported.
action.email.reportServerURL	Not supported.

Name	Description
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server.
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
action.populate_lookup	The state of the populate lookup action.
action.populate_lookup.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.populate_lookup.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.populate_lookup.maxresults	The maximum number of search results sent using alerts.
action.populate_lookup.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d]

Name	Description
action.populate_lookup.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.populate_lookup.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]
action.rss	The state of the RSS action.
action.rss.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.rss.hostname	Sets the hostname used in the web link (url) sent in alert actions.
action.rss.maxresults	Sets the maximum number of search results sent using alerts.
action.rss.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.
action.rss.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.rss.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.script	The state of the script action.
action.script.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.script.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See *action.email.hostname* for details.
action.script.maxresults	The maximum number of search results sent using alerts.

Name	Description
action.script.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted.
action.script.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.script.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.summary_index	Specifies whether the summary index action is enabled for this search.
action.summary_index._type"	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to `event` or `metric`.
action.summary_index.force_realtime_schedule	By default, *realtime_schedule* is `false` for a report configured for summary indexing. When set to `1` or `true`, this setting overrides *realtime_schedule*. Setting this setting to `true` can cause gaps in summary data, as a *realtime_schedule* search is skipped if search concurrency limits are violated.
action.summary_index.inline	Determines whether to execute the summary indexing action as part of the scheduled search. *Note:* This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).
action.summary_index.maxresults	Sets the maximum number of search results sent using alerts.
action.summary_index.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.
action.summary_index.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.summary_index.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p.
alert.digest_mode	Indicates if alert actions are applied to the entire result set or to each individual result.
alert.expires	Sets the period of time to show the alert in the dashboard. Defaults to 24h. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.managedBy	Specifies the feature or component that created the alert.
alert.severity	The alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL
alert.suppress	Indicates whether alert suppression is enabled for this scheduled search.

Name	Description
alert.suppress.fields	List of fields to use when suppressing per-result alerts. Must be specified if the digest mode is disabled and suppression is enabled.
alert.suppress.group_name	Optional setting. Used to define an alert suppression group for a set of alerts that are running over identical or very similar datasets. Alert suppression groups can help you avoid getting multiple triggered alert notifications for the same data.
alert.suppress.period	Specifies the suppression period. Only valid if alert.suppress is enabled. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.track	Specifies whether to track the actions triggered by this scheduled search. `auto` - (Default) Determine whether to apply alert tracking to this search, based on the tracking setting of each action. Do not track scheduled searches that always trigger actions. `true` - Force alert tracking for this search. Default. `false` - Disable alert tracking for this search.
alert_comparator	One of the following strings: greater than less than equal to rises by drops by rises by perc drops by perc Used with *alert_threshold* to trigger alert actions.
alert_condition	A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. *Note:* If you specify an *alert_condition*, do not set counttype, relation, or quantity.
alert_threshold	Valid values are: Integer[%] Specifies the value to compare (see *alert_comparator*) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to *rises by perc" or "drops by perc."*
alert_type	What to base the alert on, overridden by *alert_condition* if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
allow_skew	Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods. **Caution:** This setting does not require adjusting in most use cases. Check with an admin before making any updates. When set to a non-zero value for searches with the following `cron_schedule` values, the search scheduler randomly skews the second, minute, and hour

Name	Description

	on which the search runs.
	`* * * * *     Every minute.`
	`*/M * * * *   Every M minutes (M > 0).`
	`0 * * * *     Every hour.`
	`0 */H * * *   Every H hours (H > 0).`
	`0 0 * * *     Every day (at midnight).`
	When set to a non-zero value for a search that has any other `cron_schedule` setting, the search scheduler can randomly skew only the second on which the search runs.
	The amount of skew for a specific search remains constant between edits of the search.
	A value of `0` disallows skew. `0` is the default setting.
	Percentage
	`<int>` followed by `%` specifies the maximum amount of time to skew as a percentage of the scheduled search period.
	Duration
	`<int><unit>` specifies a maximum duration. The `<unit>` can be omitted only when the `<int>` is `0`.
	Valid duration units:
	• `m`
	• `min`
	• `minute`
	• `mins`
	• `minutes`
	• `h`
	• `hr`
	• `hour`
	• `hrs`
	• `hours`
	• `d`
	• `day`
	• `days`
	Examples
	`100% (for an every-5-minute search) = 5 minutes maximum`
	`50% (for an every-minute search) = 30 seconds maximum`
	`5m = 5 minutes maximum`
	`1h = 1 hour maximum`

auto_summarize	Specifies whether the search scheduler should ensure that the data for this search is automatically summarized.
auto_summarize.command	A search template to use to construct the auto-summarization for the search. Do not change.

Name	Description
auto_summarize.cron_schedule	Cron schedule to use to probe or generate the summaries for this search
auto_summarize.dispatch.<arg-name>	Dispatch options that can be overridden when running the summary search.
auto_summarize.max_concurrent	The maximum number of concurrent instances of this auto summarizing search that the scheduler is allowed to run.
auto_summarize.max_disabled_buckets	The maximum number of buckets with suspended summarization before the summarization search is completely stopped and the summarization of the search is suspended for the value specified by the *auto_summarize.suspend_period* setting.
auto_summarize.max_summary_ratio	The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket.
auto_summarize.max_summary_size	The minimum summary size, in bytes, before testing whether the summarization is helpful.
auto_summarize.max_time	The maximum time, in seconds, that the auto-summarization search is allowed to run.
auto_summarize.suspend_period	The amount of time to suspend summarization of the search if the summarization is deemed unhelpful.
auto_summarize.timespan	Comma-delimited list of time ranges that each summarized chunk should span. Comprises the list of available summary ranges for which summaries would be available. Does not support `1w` timespans.
auto_summarize.workload_pool	Sets the name of the workload pool that is used by the auto-summarization of this search.
cron_schedule	The cron schedule to run this search. For more information, refer to the description of this parameter in the POST endpoint.
defer_scheduled_searchable_idxc	Specifies whether to defer a continuous saved search during a searchable rolling restart or searchable rolling upgrade of an indexer cluster.
description	Human-readable description of this saved search.
disabled	Indicates whether this saved search is disabled.
dispatch.allow_partial_results	Specifies whether the search job can proceed to provide partial results if a search peer fails. When set to false, the search job fails if a search peer providing results for the search job fails.
dispatch.auto_cancel	Specifies the amount of inactive time, in seconds, after which the search job is automatically canceled.
dispatch.auto_pause	Specifies the amount of inactive time, in seconds, after which the search job is automatically paused.
dispatch.buckets	The maximum number of timeline buckets.
dispatch.earliest_time	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.index_earliest	Specifies the earliest index time for this search. Can be a relative or absolute time.
dispatch.index_latest	Specifies the latest index time for this saved search. Can be a relative or absolute time.
dispatch.indexedRealtime	Specifies whether to use 'indexed-realtime' mode when doing real-time searches.
dispatch.indexedRealtimeMinSpan	Specifies the minimum number of seconds to wait between component index searches.
dispatch.indexedRealtimeOffset	Specifies the number of seconds to wait for disk flushes to finish.
dispatch.indexedRealtimeMinSpan	Allows for a per-job override of the `[search] indexed_realtime_default_span` setting in `limits.conf`. The default for saved searches is "unset", falling back to the `limits.conf` setting.

Name	Description
dispatch.latest_time	A time string that specifies the latest time for the saved search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.lookups	Indicates if lookups are enabled for this search.
dispatch.max_count	The maximum number of results before finalizing the search.
dispatch.max_time	Indicates the maximum amount of time (in seconds) before finalizing the search.
dispatch.reduce_freq	Specifies how frequently the MapReduce reduce phase runs on accumulated map values.
dispatch.rt_backfill	Specifies whether to do real-time window backfilling for scheduled real-time searches.
dispatch.rt_maximum_span	Sets the maximum number of seconds to search data that falls behind real time.
dispatch.sample_ratio	The integer value used to calculate the sample ratio. The formula is `1 / <integer>`.
dispatch.spawn_process	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Specifies whether new search process is spawned when this saved search is executed. Searches against indexes must run in a separate process.
dispatch.time_format	Time format string that defines the time format for specifying the earliest and latest time.
dispatch.ttl	Indicates the time to live (ttl), in seconds, for the artifacts of the scheduled search, if no actions are triggered.
dispatchAs	When the saved search is dispatched using the "saved/searches/{name}/dispatch" endpoint, this setting controls what user that search is dispatched as. Only meaningful for shared saved searches. Can be set to `owner` or `user`.
displayview	Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.
durable.backfill_type	Specifies how the Splunk software backfills the lost search results of failed scheduled search jobs. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type.* Valid values are `auto`, `time_interval`, and `time_whole`.
durable.lag_time	Specifies the search time delay, in seconds, that a durable search uses to catch events that are ingested or indexed late. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.max_backfill_intervals	Specifies the maximum number of cron intervals (previous scheduled search jobs) that the Splunk software can attempt to backfill for this search, when those jobs have incomplete events. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type.*
durable.track_time_type	Indicates that a scheduled search is durable and specifies how the search tracks events. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
earliest_time	For scheduled searches display all the scheduled times starting from this time (not just the next run time).
is_scheduled	Indicates if this search is to be run on a schedule
is_visible	Indicates if this saved search appears in the visible saved search list.
latest_time	For scheduled searches display all the scheduled times until this time (not just the next run time).

Name	Description
listDefaultActionArgs	List default values of *actions.**, even though some of the actions may not be specified in the saved search.
max_concurrent	The maximum number of concurrent instances of this search the scheduler is allowed to run.
next_scheduled_time	Time when the scheduler runs this search again.
orphan	If `add_orphan_field` has been specified in the GET request, indicates whether the search is orphaned.
qualifiedSearch	The exact search string that the scheduler would run.
realtime_schedule	Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. See the POST parameter for this attribute for details.
request.ui_dispatch_app	A field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	Specifies a field used by Splunk Web to denote the view this search should be displayed in.
restart_on_searchpeer_add	Specifies whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. *Note:* The peer can be a newly added peer or a peer down and now available.
run_n_times	Runs this search exactly the specified number of times. Does not run the search again until the Splunk platform is restarted.
run_on_startup	Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Defaults to 0. This parameter should be set to 1 for scheduled searches that populate lookup tables.

schedule_priority	Indicates the scheduling priority of a specific search. One of the following values.
	`[ default | higher | highest ]`
	default
	No scheduling priority increase.
	higher
	Scheduling priority is higher than other searches of the same scheduling tier. While there are four tiers of priority for scheduled searches, only the following are affected by this property:
	`* real-Time-Scheduled (realtime_schedule=1).`
	`* continuous-Scheduled (realtime_schedule=0).`
	highest
	Scheduling priority is higher than other searches regardless of scheduling tier. However, real-time-scheduled searches with `priority = highest` always have priority over continuous scheduled searches with `priority = highest`.
	This is the high-to-low priority order (where RTSS = real-time-scheduled search, CSS = continuous-scheduled search, d = default, h = higher, H =

Name	Description
	highest). `RTSS(H) > CSS(H) > RTSS(h) > RTSS(d) > CSS(h) > CSS(d)` Changing the priority requires the search owner to have the `edit_search_schedule_priority` capability in order to make non-default settings. Defaults to `default`. For more details, see `savedsearches.conf.spec`.
schedule_window	Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to `auto`, the scheduler prioritizes searches automatically.
search	Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has "foo" as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.
vsid	The viewstate id associated with the UI view listed in 'displayview'. Must match up to a stanza in viewstates.conf.

Example requests and responses

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/saved/searches
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://fool01:8092/services/saved/searches</id>
  <updated>2021-04-29T09:22:44-07:00</updated>
  <generator build="84cbec3d51a6" version="8.2.2105"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <link href="/services/saved/searches/_acl" rel="_acl"/>
  <opensearch:totalResults>8</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Errors in the last 24 hours</title>
    <id>https://fool01:8092/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours<
```

```
/id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours"
rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours" rel="list"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/disable"
rel="disable"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/dispatch"
rel="dispatch"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/embed"
rel="embed"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/history"
rel="history"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">0</s:key>
        <s:key name="action.email.sendresults"></s:key>
        <s:key name="action.email.to"></s:key>
        <s:key name="action.populate_lookup">0</s:key>
        <s:key name="action.rss">0</s:key>
        <s:key name="action.script">0</s:key>
        <s:key name="action.summary_index">0</s:key>
        <s:key name="action.summary_index.force_realtime_schedule">0</s:key>
        <s:key name="actions"></s:key>
        <s:key name="alert.digest_mode">1</s:key>
        <s:key name="alert.expires">24h</s:key>
        <s:key name="alert.managedBy"></s:key>
        <s:key name="alert.severity">3</s:key>
        <s:key name="alert.suppress"></s:key>
        <s:key name="alert.suppress.fields"></s:key>
        <s:key name="alert.suppress.group_name"></s:key>
        <s:key name="alert.suppress.period"></s:key>
        <s:key name="alert.track">0</s:key>
        <s:key name="alert_comparator"></s:key>
        <s:key name="alert_condition"></s:key>
        <s:key name="alert_threshold"></s:key>
        <s:key name="alert_type">always</s:key>
        <s:key name="allow_skew">0</s:key>
        <s:key name="auto_summarize">0</s:key>
        <s:key name="auto_summarize.command"><![CDATA[| summarize override=partial
timespan=$auto_summarize.timespan$ max_summary_size=$auto_summarize.max_summary_size$
max_summary_ratio=$auto_summarize.max_summary_ratio$
max_disabled_buckets=$auto_summarize.max_disabled_buckets$ max_time=$auto_summarize.max_time$ [ $search$
]]]></s:key>
        <s:key name="auto_summarize.cron_schedule">*/10 * * * *</s:key>
        <s:key name="auto_summarize.dispatch.earliest_time"></s:key>
        <s:key name="auto_summarize.dispatch.latest_time"></s:key>
        <s:key name="auto_summarize.dispatch.time_format">%FT%T.%Q%:z</s:key>
        <s:key name="auto_summarize.dispatch.ttl">60</s:key>
        <s:key name="auto_summarize.max_concurrent">1</s:key>
        <s:key name="auto_summarize.max_disabled_buckets">2</s:key>
        <s:key name="auto_summarize.max_summary_ratio">0.1</s:key>
        <s:key name="auto_summarize.max_summary_size">52428800</s:key>
        <s:key name="auto_summarize.max_time">3600</s:key>
        <s:key name="auto_summarize.suspend_period">24h</s:key>
        <s:key name="auto_summarize.timespan"></s:key>
```

```
<s:key name="auto_summarize.workload_pool"></s:key>
<s:key name="cron_schedule"></s:key>
<s:key name="defer_scheduled_searchable_idxc">0</s:key>
<s:key name="description"></s:key>
<s:key name="disabled">0</s:key>
<s:key name="dispatch.allow_partial_results">1</s:key>
<s:key name="dispatch.auto_cancel">0</s:key>
<s:key name="dispatch.auto_pause">0</s:key>
<s:key name="dispatch.buckets">0</s:key>
<s:key name="dispatch.earliest_time">-1d</s:key>
<s:key name="dispatch.index_earliest"></s:key>
<s:key name="dispatch.index_latest"></s:key>
<s:key name="dispatch.indexedRealtime"></s:key>
<s:key name="dispatch.indexedRealtimeMinSpan"></s:key>
<s:key name="dispatch.indexedRealtimeOffset"></s:key>
<s:key name="dispatch.latest_time"></s:key>
<s:key name="dispatch.lookups">1</s:key>
<s:key name="dispatch.max_count">500000</s:key>
<s:key name="dispatch.max_time">0</s:key>
<s:key name="dispatch.reduce_freq">10</s:key>
<s:key name="dispatch.rt_backfill">0</s:key>
<s:key name="dispatch.rt_maximum_span"></s:key>
<s:key name="dispatch.sample_ratio">1</s:key>
<s:key name="dispatch.spawn_process">1</s:key>
<s:key name="dispatch.time_format">%FT%T.%Q%:z</s:key>
<s:key name="dispatch.ttl">2p</s:key>
<s:key name="dispatchAs">owner</s:key>
<!-- display settings elided-->
<s:key name="displayview"></s:key>
<s:key name="durable.backfill_type">auto</s:key>
<s:key name="durable.lag_time">0</s:key>
<s:key name="durable.max_backfill_intervals">0</s:key>
<s:key name="durable.track_time_type"></s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">search</s:key>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">0</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">nobody</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>admin</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">app</s:key>
  </s:dict>
</s:key>
```

```
        <s:key name="embed.enabled">0</s:key>
        <s:key name="federated.provider"></s:key>
        <s:key name="is_scheduled">0</s:key>
        <s:key name="is_visible">1</s:key>
        <s:key name="max_concurrent">1</s:key>
        <s:key name="next_scheduled_time"></s:key>
        <s:key name="qualifiedSearch">search error OR failed OR severe OR ( sourcetype=access_* ( 404 OR
500 OR 503 ) )</s:key>
        <s:key name="realtime_schedule">1</s:key>
        <s:key name="request.ui_dispatch_app"></s:key>
        <s:key name="request.ui_dispatch_view"></s:key>
        <s:key name="restart_on_searchpeer_add">1</s:key>
        <s:key name="run_n_times">0</s:key>
        <s:key name="run_on_startup">0</s:key>
        <s:key name="schedule_as">auto</s:key>
        <s:key name="schedule_priority">default</s:key>
        <s:key name="schedule_window">0</s:key>
        <s:key name="search">error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503 )
)</s:key>
        <s:key name="skip_scheduled_realtime_idxc">0</s:key>
        <s:key name="vsid"></s:key>
        <s:key name="workload_pool"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create a saved search.

Request parameters

Name	Type	Description
action.<action_name>	Boolean	Enable or disable an alert action. See `alert_actions.conf` for available alert action types. `action_name` defaults to an empty string.
action.<action_name>.<parameter>		Use this syntax to configure action parameters. See `alert_actions.conf` for parameter options.
action.summary_index._type"	String	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to `event` or `metric`.
action.summary_index.force_realtime_schedule	Boolean	By default, *realtime_schedule* is `false` for a report configured for summary indexing. When set to `1` or `True`, this setting overrides *realtime_schedule*. Setting this setting to `true` can cause gaps in summary data, as a *realtime_schedule* search is skipped if search concurrency limits are violated.
actions	String	A comma-separated list of actions to enable. For example: rss,email
alert.digest_mode	Boolean	Specifies whether alert actions are applied to the entire result set or on each individual result. Defaults to 1.
alert.expires	Number	Valid values: [number][time-unit]

Name	Type	Description
		Sets the period of time to show the alert in the dashboard. Defaults to 24h. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.severity	Enum	Valid values: (1 | 2 | 3 | 4 | 5 | 6) Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN (default) 4 ERROR 5 SEVERE 6 FATAL
alert.suppress	Boolean	Indicates whether alert suppression is enabled for this scheduled search.
alert.suppress.fields	String	Comma delimited list of fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
alert.suppress.group_name	String	Optional setting. Used to define an alert suppression group for a set of alerts that are running over identical or very similar datasets. Alert suppression groups can help you avoid getting multiple triggered alert notifications for the same data.
alert.suppress.period	Number	Valid values: [number][time-unit] Specifies the suppression period. Only valid if *alert.suppress* is enabled. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.track	String	Valid values: (true | false | auto) Specifies whether to track the actions triggered by this scheduled search. `auto` - Determine whether to apply alert tracking to this search, based on the tracking setting of each action. Do not track scheduled searches that always trigger actions. Default. `true` - Force alert tracking for this search. `false` - Disable alert tracking for this search.
alert_comparator	String	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc. Used with *alert_threshold* to trigger alert actions.
alert_condition	String	Contains a conditional search that is evaluated against the results of the saved search. Defaults to an empty string.

Name	Type	Description
		Alerts are triggered if the specified search yields a non-empty search result list. **Note:** If you specify an alert_condition, do not set counttype, relation, or quantity.
alert_threshold	Number	Valid values are: Integer[%] Specifies the value to compare (see *alert_comparator*) before triggering the alert actions. If expressed as a percentage, indicates value to use when *alert_comparator* is set to "rises by perc" or "drops by perc."
alert_type	String	What to base the alert on, overridden by *alert_condition* if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.

allow_skew	`0 |`
	`<percentage> |`
	`<duration>`
		Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods. Defaults to `0` (skew disabled).
		Caution: This setting does not require adjusting in most use cases. Check with an admin before making any updates.
		When set to a non-zero value for searches with the following *cron_schedule' values, the search scheduler randomly skews the second, minute, and hour on which the search runs.*
		`* * * * *     Every minute.`
		`*/M * * * *   Every M minutes (M > 0).`
		`0 * * * *     Every hour.`
		`0 */H * * *   Every H hours (H > 0).`
		`0 0 * * *     Every day (at midnight).`
		When set to a non-zero value for a search that has any other `cron_schedule` setting, the search scheduler can randomly skew only the second on which the search runs.
		The amount of skew for a specific search remains constant between edits of the search.
		A value of `0` disallows skew. `0` is the default setting.
		Percentage
		`<int>` followed by `%` specifies the maximum amount of time to skew as a percentage of the scheduled search period.
		Duration
		`<int><unit>` specifies a maximum duration. The `<unit>` can be omitted only when the `<int>` is `0`.

Name	Type	Description

		Valid duration units:
		• `m`
		• `min`
		• `minute`
		• `mins`
		• `minutes`
		• `h`
		• `hr`
		• `hour`
		• `hrs`
		• `hours`
		• `d`
		• `day`
		• `days`
		Examples
		`100% (for an every-5-minute search) = 5 minutes maximum`
		`50% (for an every-minute search) = 30 seconds maximum`
		`5m = 5 minutes maximum`
		`1h = 1 hour maximum`

*args.**	String	Wildcard argument that accepts any saved search template argument, such as args.username=foobar when the search is search $username$.
auto_summarize	Boolean	Indicates whether the scheduler should ensure that the data for this search is automatically summarized. Defaults to 0.
auto_summarize.command	String	An auto summarization template for this search. See auto summarization options in `savedsearches.conf` for more details. Do not change unless you understand the architecture of saved search auto summarization.
auto_summarize.cron_schedule	String	Cron schedule that probes and generates the summaries for this saved search. The default value, `*/10 * * * *`, corresponds to "every ten hours".
auto_summarize.dispatch.earliest_time	String	A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
auto_summarize.dispatch.latest_time	String	A time string that specifies the latest time for summarizing this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
auto_summarize.dispatch.time_format	String	Defines the time format used to specify the earliest and latest time. Defaults to `%FT%T.%Q%:z`

Name	Type	Description
auto_summarize.dispatch.ttl	String	Valid values: Integer[p] Indicates the time to live (ttl), in seconds, for the artifacts of the summarization of the scheduled search. Defaults to 60.
auto_summarize.max_concurrent	Number	The maximum number of concurrent instances of this auto summarizing search that the scheduler is allowed to run.
auto_summarize.max_disabled_buckets	Number	The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for auto_summarize.suspend_period. Defaults to 2.
auto_summarize.max_summary_ratio	Number	The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. Defaults to 0.1. *Note:* The test is only performed if the summary size is larger than auto_summarize.max_summary_size.
auto_summarize.max_summary_size	Number	The minimum summary size, in bytes, before testing whether the summarization is helpful. The default value, `52428800`, is equivalent to 5MB.
auto_summarize.max_time	Number	The maximum time, in seconds, that the summary search is allowed to run. Defaults to 3600. *Note:* This is an approximate time. The summary search stops at clean bucket boundaries.
auto_summarize.suspend_period	String	The amount of time to suspend summarization of this search if the summarization is deemed unhelpful. Defaults to 24h.
auto_summarize.timespan	String	Comma-delimited list of time ranges that each summarized chunk should span. Comprises the list of available granularity levels for which summaries would be available. Does not support `1w` timespans. For example, a timechart over the last month whose granularity is at the day level should set this to `1d`. If you need the same data summarized at the hour level for weekly charts, use: `1h,1d`.
cron_schedule	String	Valid values: cron string The cron schedule to execute this search. For example: `*/5 * * * *` causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: `00,20,40 * * * *`, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of `03,23,43 * * * *` runs the search every hour at hh:03, hh:23, hh:43.

Name	Type	Description
		To reduce system load, schedule your searches so that they are staggered over time. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.
description	String	Human-readable description of this saved search. Defaults to empty string.
disabled	Boolean	Indicates whether the saved search is enabled. Defaults to 0. Disabled saved searches are not visible in Splunk Web.
*dispatch.**	String	Wildcard argument that accepts any dispatch related argument.
dispatch.allow_partial_results	Boolean	Specifies whether the search job can proceed to provide partial results if a search peer fails. When set to false, the search job fails if a search peer providing results for the search job fails.
dispatch.auto_cancel	Number	Specifies the amount of inactive time, in seconds, after which the search job is automatically canceled.
dispatch.auto_pause	Number	Specifies the amount of inactive time, in seconds, after which the search job is automatically paused.
dispatch.buckets	Number	The maximum number of timeline buckets. Defaults to 0.
dispatch.earliest_time	String	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.index_earliest	String	A time string that specifies the earliest index time for this search. Can be a relative or absolute time.
dispatch.index_latest	String	A time string that specifies the latest index time for this saved search. Can be a relative or absolute time.
dispatch.indexedRealtime	Boolean	Indicates whether to used indexed-realtime mode when doing real-time searches.
dispatch.indexedRealtimeOffset	Number	Allows for a per-job override of the `[search] indexed_realtime_disk_sync_delay` setting in `limits.conf`. Default for saved searches is "unset", falling back to `limits.conf` setting.
dispatch.indexedRealtimeMinSpan	Number	Allows for a per-job override of the `[search] indexed_realtime_default_span` setting in `limits.conf`. Default for saved searches is "unset", falling back to the `limits.conf` setting.
dispatch.latest_time	String	A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.lookups	Boolean	Enables or disables the lookups for this search. Defaults to 1.
dispatch.max_count	Number	The maximum number of results before finalizing the search. Defaults to 500000.
dispatch.max_time	Number	

Name	Type	Description
		Indicates the maximum amount of time (in seconds) before finalizing the search. Defaults to 0.
dispatch.reduce_freq	Number	Specifies, in seconds, how frequently the MapReduce reduce phase runs on accumulated map values. Defaults to 10.
dispatch.rt_backfill	Boolean	Whether to back fill the real time window for this search. Parameter valid only if this is a real time search. Defaults to 0.
dispatch.rt_maximum_span	Number	Allows for a per-job override of the `[search] indexed_realtime_maximum_span` setting in `limits.conf`. Default for saved searches is "unset", falling back to the `limits.conf` setting.
dispatch.sample_ratio	Number	The integer value used to calculate the sample ratio. The formula is `1 / <integer>`.
dispatch.spawn_process	Boolean	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Specifies whether to spawn a new search process when this saved search is executed. Defaults to 1. Searches against indexes *must* run in a separate process.
dispatch.time_format	String	A time format string that defines the time format for specifying the earliest and latest time. Defaults to `%FT%T.%Q%:z`.
dispatch.ttl	Number	Valid values: Integer[p]. Defaults to 2p. Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered. If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to `alert_actions.conf.spec`. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.
dispatchAs	String	When the saved search is dispatched using the "saved/searches/{name}/dispatch" endpoint, this setting controls what user that search is dispatched as. Only meaningful for shared saved searches. Can be set to `owner` or `user`.
displayview	String	Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.
durable.backfill_type	String	Specifies how the Splunk software backfills the lost search results of failed scheduled search jobs. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*. Valid values are `auto`, `time_interval`, and `time_whole`.

Name	Type	Description
		`time_whole` - The Splunk software schedules a single backfill search job with a time range that spans the combined time ranges of all failed scheduled search jobs. The `time_whole` setting can be applied only to searches that are streaming, where the results are raw events without additional aggregation. `time_interval` - The Splunk software schedules multiple backfill search jobs, one for each failed scheduled search job. The backfill jobs have time ranges that match those of the failed jobs. The `time_interval` setting can be applied to both streaming and non-streaming searches. `auto` - The Splunk software decides the backfill type by checking whether the search is streaming or not. If the search is streaming, the Splunk software uses the `time_whole` backfill type. Otherwise, it uses the `time_interval` backfill type.
durable.lag_time	Number	Specifies the search time delay, in seconds, that a durable search uses to catch events that are ingested or indexed late. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.max_backfill_intervals	Number	Specifies the maximum number of cron intervals (previous scheduled search jobs) that the Splunk software can attempt to backfill for this search, when those jobs have incomplete events. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.track_time_type	String	Indicates that a scheduled search is durable and specifies how the search tracks events. A durable search is a search that tries to ensure the delivery of all results, even when the search process is slowed or stopped by runtime issues like rolling restarts, network bottlenecks, and even downed servers. Applies only to scheduled searches. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
is_scheduled	Boolean	Whether this search is to be run on a schedule
is_visible	Boolean	Specifies whether this saved search should be listed in the visible saved search list. Defaults to 1.
max_concurrent	Number	The maximum number of concurrent instances of this search the scheduler is allowed to run. Defaults to 1.
name	String	**Required**. A name for the search.
next_scheduled_time	String	Read-only attribute. Value ignored on POST. There are some old clients who still send this value

Name	Type	Description
qualifiedSearch	String	Read-only attribute. Value ignored on POST. This value is computed during runtime.
realtime_schedule	Boolean	Controls the way the scheduler computes the next execution time of a scheduled search. Defaults to 1. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).
request.ui_dispatch_app	String	Specifies a field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	String	Specifies a field used by Splunk Web to denote the view this search should be displayed in.
restart_on_searchpeer_add	Boolean	Specifies whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. Defaults to 1. **Note:** The peer can be a newly added peer or a peer down and now available.
run_n_times	Number	Runs this search exactly the specified number of times. Does not run the search again until the Splunk platform is restarted.
run_on_startup	Boolean	Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Defaults to 0. Set *run_on_startup* to `1` for scheduled searches that populate lookup tables.
schedule_priority	String	Configures the scheduling priority of a specific search. One of the following values. `[ default | higher | highest ]` default No scheduling priority increase. higher Scheduling priority is higher than other searches of the same scheduling tier. While there are four tiers of priority for scheduled searches, only the following are affected by this property:

Name	Type	Description

		`* real-Time-Scheduled (realtime_schedule=1).`
		`* continuous-Scheduled (realtime_schedule=0).`
		highest
		Scheduling priority is higher than other searches regardless of scheduling tier. However, real-time-scheduled searches with `priority = highest` always have priority over continuous scheduled searches with `priority = highest`.
		This is the high-to-low priority order (where RTSS = real-time-scheduled search, CSS = continuous-scheduled search, d = default, h = higher, H = highest).
		`RTSS(H) > CSS(H) > RTSS(h) > RTSS(d) > CSS(h) > CSS(d)`
		Changing the priority requires the search owner to have the `edit_search_schedule_priority` capability in order to make non-default settings.
		Defaults to `default`.
		For more details, see `savedsearches.conf.spec`.

schedule_window	Number or `auto`	Time window (in minutes) during which the search has lower priority. Defaults to 0. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. Set to `auto` to let the scheduler determine the optimal window value automatically. Requires the `edit_search_schedule_window` capability to override `auto`.
search	String	**Required**. The search to save.
vsid	String	Defines the viewstate id associated with the UI view listed in 'displayview'. Must match up to a stanza in viewstates.conf.
workload_pool	String	Specifies the new workload pool where the existing running search will be placed.

Returned values

Name	Description
action.<action_name>	Indicates whether the `<action_name>` is enabled or disabled for a particular search. For more information about the alert action options see the `alert_actions.conf` file.
action.<action_name>.<parameter>	Overrides the setting defined for an action in the `alert_actions.conf` file with a new setting that is valid only for the search configuration to which it is applied.
action.email	Indicates the state of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the

Name	Description
	next restart. Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.email.format	Specify the format of text in the email. This value also applies to any attachments.< Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates. Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf.
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct a url that can be referenced externally, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails.

Name	Description
	Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the global maximum number of search results to send when email.action is enabled.
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.pdfview	The name of the view to deliver if sendpdf is enabled
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportCIDFontList	Space-separated list. Specifies the set (and load order) of CID fonts for handling Simplified Chinese(gb), Traditional Chinese(cns), Japanese(jp), and Korean(kor) in Integrated PDF Rendering. If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used. To skip loading any CID fonts, specify the empty string. Default value: "gb cns jp kor"
action.email.reportIncludeSplunkLogo	Indicates whether to include the Splunk logo with the report.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.reportServerEnabled	Not supported.
action.email.reportServerURL	Not supported.
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server.

Name	Description
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
action.email.width_sort_columns	Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.
action.populate_lookup	Indicates the state of the populate lookup action.
action.populate_lookup.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.populate_lookup.dest	Lookup name of path of the lookup to populate.
action.populate_lookup.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.populate_lookup.maxresults	The maximum number of search results sent using alerts.
action.populate_lookup.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d]
action.populate_lookup.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.populate_lookup.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]
action.rss	Indicates the state of the RSS action.
action.rss.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.rss.hostname	Sets the hostname used in the web link (url) sent in alert actions.

Name	Description
	This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.rss.maxresults	Sets the maximum number of search results sent using alerts.
action.rss.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Valid values are Integer[m |s |h |d].
action.rss.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.rss.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.script	Indicates the state of the script for this action.
action.script.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.script.filename	File name of the script to call. Required if script action is enabled
action.script.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.script.maxresults	Sets the maximum number of search results sent using alerts.
action.script.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted.
action.script.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.script.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes).

Name	Description
	If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.summary_index	Indicates the state of the summary index.
action.summary_index._name	Specifies the name of the summary index where the results of the scheduled search are saved. Defaults to "summary."
action.summary_index.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.summary_index.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.summary_index.inline	Determines whether to execute the summary indexing action as part of the scheduled search. *Note:* This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).
action.summary_index.maxresults	Sets the maximum number of search results sent using alerts.
action.summary_index.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d]
action.summary_index.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.summary_index.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
actions	Actions triggerd by this alert.
alert.digest_mode	Indicates if the alert actions are applied to the entire result set or to each individual result.
alert.expires	Sets the period of time to show the alert in the dashboard. Defaults to 24h.

Name	Description
	Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour. Valid values: [number][time-unit]
alert.severity	Valid values: (1 | 2 | 3 | 4 | 5 | 6) Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL
alert.suppress	Indicates whether alert suppression is enabled for this schedules search.
alert.suppress.fields	Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
alert.suppress.period	Specifies the suppresion period. Only valid if alert.supress is enabled. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.track	Specifies whether to track the actions triggered by this scheduled search. auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions. true - force alert tracking. false - disable alert tracking for this search.
alert_comparator	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc
alert_condition	A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. *Note:* If you specify an alert_condition, do not set counttype, relation, or quantity.
alert_threshold	Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to "rises by perc" or "drops by perc."
alert_type	What to base the alert on, overriden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.

Name	Description

allow_skew	`0 | <percentage> | <duration>`
	Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.
	Caution: This setting does not require adjusting in most use cases. Check with an admin before making any updates.
	When set to a non-zero value for searches with the following `cron_schedule` values, the search scheduler randomly skews the second, minute, and hour on which the search runs.
	`* * * * *     Every minute.`
	`*/M * * * *   Every M minutes (M > 0).`
	`0 * * * *     Every hour.`
	`0 */H * * *   Every H hours (H > 0).`
	`0 0 * * *     Every day (at midnight).`
	When set to a non-zero value for a search that has any other `cron_schedule` setting, the search scheduler can randomly skew only the second on which the search runs.
	The amount of skew for a specific search remains constant between edits of the search.
	A value of `0` disallows skew. `0` is the default setting.
	Percentage
	`<int>` followed by `%` specifies the maximum amount of time to skew as a percentage of the scheduled search period.
	Duration
	`<int><unit>` specifies a maximum duration. The `<unit>` can be omitted only when the `<int>` is `0` (which disables skew).
	Valid duration units:
	• `m`
	• `min`
	• `minute`
	• `mins`
	• `minutes`
	• `h`
	• `hr`
	• `hour`
	• `hrs`
	• `hours`
	• `d`
	• `day`
	• `days`
	Examples

Name	Description
	100% (for an every-5-minute search) = 5 minutes maximum 50% (for an every-minute search) = 30 seconds maximum 5m = 5 minutes maximum 1h = 1 hour maximum
*args.**	Wildcard argument that accepts any saved search template argument, such as args.username=foobar when the search is search $username$.
auto_summarize	Indicates whether the scheduler should ensure that the data for this search is automatically summarized.
auto_summarize.command	A search template that constructs the auto summarization for this search. **Caution:** Advanced feature. Do not change unless you understand the architecture of auto summarization of saved searches.
auto_summarize.cron_schedule	Cron schedule that probes and generates the summaries for this saved search.
auto_summarize.dispatch.earliest_time	A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time.
auto_summarize.dispatch.latest_time	A time string that specifies the latest time for this saved search. Can be a relative or absolute time.
auto_summarize.dispatch.time_format	Time format used to specify the earliest and latest times.
auto_summarize.dispatch.ttl	Indicates the time to live (in seconds) for the artifacts of the summarization of the scheduled search. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.
auto_summarize.max_disabled_buckets	The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for auto_summarize.suspend_period.
auto_summarize.max_summary_ratio	The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. *Note:* The test is only performed if the summary size is larger than auto_summarize.max_summary_size.
auto_summarize.max_summary_size	The minimum summary size, in bytes, before testing whether the summarization is helpful.
auto_summarize.max_time	Maximum time (in seconds) that the summary search is allowed to run. *Note:* This is an approximate time. The summary search stops at clean bucket boundaries.
auto_summarize.suspend_period	Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful.
auto_summarize.timespan	The list of time ranges that each summarized chunk should span. This comprises the list of available granularity levels for which summaries would be available. For example a timechart over the last month whose granularity is at the day level should set this to 1d. If you need the same data summarized at the hour level for weekly charts, use: 1h,1d.
cron_schedule	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.

Name	Description
	cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string
description	Description of this saved search. Defaults to empty string.
disabled	Indicates if this saved search is disabled.
*dispatch.**	* represents any custom dispatch field.
dispatch.buckets	The maximum nuber of timeline buckets.
dispatch.earliest_time	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
dispatch.indexedRealtime	Indicates whether to used indexed-realtime mode when doing real-time searches.
dispatch.latest_time	A time string that specifies the latest time for the saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
dispatch.lookups	Indicates if lookups are enabled for this search.
dispatch.max_count	The maximum number of results before finalizing the search.
dispatch.max_time	Indicates the maximum amount of time (in seconds) before finalizing the search.
dispatch.reduce_freq	Specifies how frequently the MapReduce reduce phase runs on accumulated map values.
dispatch.rt_backfill	Indicates whether to back fill the real time window for this search. Parameter valid only if this is a real time search
dispatch.spawn_process	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Indicates whether a new search process spawns when this saved search is executed.
dispatch.time_format	Time format string that defines the time format for specifying the earliest and latest time.
dispatch.ttl	Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered. If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to `alert_actions.conf.spec`. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.

Name	Description
displayview	Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.
durable.backfill_type	Specifies how the Splunk software backfills the lost search results of failed scheduled search jobs. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*. Valid values are `auto`, `time_interval`, and `time_whole`.
durable.lag_time	Specifies the search time delay, in seconds, that a durable search uses to catch events that are ingested or indexed late. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.max_backfill_intervals	Specifies the maximum number of cron intervals (previous scheduled search jobs) that the Splunk software can attempt to backfill for this search, when those jobs have incomplete events. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.track_time_type	Indicates that a scheduled search is durable and specifies how the search tracks events. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
is_scheduled	Indicates if this search is to be run on a schedule.
is_visible	Indicates if this saved search appears in the visible saved search list.
max_concurrent	The maximum number of concurrent instances of this search the scheduler is allowed to run.
next_scheduled_time	The time when the scheduler runs this search again.
qualifiedSearch	The exact search string that the scheduler would run.
realtime_schedule	Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).
request.ui_dispatch_app	A field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	Specifies a field used by Splunk Web to denote the view this search should be displayed in.
restart_on_searchpeer_add	Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. *Note:* The peer can be a newly added peer or a peer down and now available.
run_on_startup	Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time.

Name	Description
	Splunk recommends that you set run_on_startup to true for scheduled searches that populate lookup tables.
schedule_window	Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to `auto`, the scheduler prioritizes searches automatically.
search	Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has "foo" as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.
vsid	The viewstate id associated with the UI view listed in 'displayview'. Matches to a stanza in viewstates.conf.

Example request and response

XML Request

```
curl -k -u admin:chang2me https://fool01:8092/services/saved/searches/ \
 -d name=test_durable \
 -d cron_schedule="*/3 * * * *" \
 -d description="This test job is a durable saved search" \
 -d dispatch.earliest_time="-24h@h" -d dispatch.latest_time=now \
 --data-urlencode search="search index="_internal" | stats count by host" \
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://fool01:8092/services/saved/searches</id>
  <updated>2021-04-29T09:56:53-07:00</updated>
  <generator build="84cbec3d51a6" version="8.2.2105"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <link href="/services/saved/searches/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>test_durable</title>
    <id>https://fool01:8092/servicesNS/admin/search/saved/searches/test_durable</id>
    <updated>2021-04-29T09:56:53-07:00</updated>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="list"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/embed" rel="embed"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/history" rel="history"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">0</s:key>
        <!-- action settings elided -->
        <s:key name="alert.digest_mode">1</s:key>
        <s:key name="alert.expires">24h</s:key>
        <s:key name="alert.managedBy"></s:key>
        <s:key name="alert.severity">3</s:key>
        <s:key name="alert.suppress"></s:key>
        <s:key name="alert.suppress.fields"></s:key>
        <s:key name="alert.suppress.group_name"></s:key>
        <s:key name="alert.suppress.period"></s:key>
        <s:key name="alert.track">0</s:key>
        <s:key name="alert_comparator"></s:key>
        <s:key name="alert_condition"></s:key>
        <s:key name="alert_threshold"></s:key>
        <s:key name="alert_type">always</s:key>
        <s:key name="allow_skew">0</s:key>
        <s:key name="auto_summarize">0</s:key>
        <s:key name="auto_summarize.command"><![CDATA[| summarize override=partial
timespan=$auto_summarize.timespan$ max_summary_size=$auto_summarize.max_summary_size$
max_summary_ratio=$auto_summarize.max_summary_ratio$
max_disabled_buckets=$auto_summarize.max_disabled_buckets$ max_time=$auto_summarize.max_time$ [ $search$
]]]></s:key>
        <s:key name="auto_summarize.cron_schedule">*/10 * * * *</s:key>
        <s:key name="auto_summarize.dispatch.earliest_time"></s:key>
        <s:key name="auto_summarize.dispatch.latest_time"></s:key>
        <s:key name="auto_summarize.dispatch.time_format">%FT%T.%Q%:z</s:key>
        <s:key name="auto_summarize.dispatch.ttl">60</s:key>
        <s:key name="auto_summarize.max_concurrent">1</s:key>
        <s:key name="auto_summarize.max_disabled_buckets">2</s:key>
        <s:key name="auto_summarize.max_summary_ratio">0.1</s:key>
        <s:key name="auto_summarize.max_summary_size">52428800</s:key>
        <s:key name="auto_summarize.max_time">3600</s:key>
        <s:key name="auto_summarize.suspend_period">24h</s:key>
        <s:key name="auto_summarize.timespan"></s:key>
        <s:key name="auto_summarize.workload_pool"></s:key>
        <s:key name="cron_schedule">*/3 * * * *</s:key>
        <s:key name="defer_scheduled_searchable_idxc">0</s:key>
        <s:key name="description">This test job is a durable saved search</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="dispatch.allow_partial_results">1</s:key>
        <s:key name="dispatch.auto_cancel">0</s:key>
        <s:key name="dispatch.auto_pause">0</s:key>
        <s:key name="dispatch.buckets">0</s:key>
        <s:key name="dispatch.earliest_time">-24h@h</s:key>
        <s:key name="dispatch.index_earliest"></s:key>
        <s:key name="dispatch.index_latest"></s:key>
        <s:key name="dispatch.indexedRealtime"></s:key>
        <s:key name="dispatch.indexedRealtimeMinSpan"></s:key>
        <s:key name="dispatch.indexedRealtimeOffset"></s:key>
        <s:key name="dispatch.latest_time">now</s:key>
        <s:key name="dispatch.lookups">1</s:key>
        <s:key name="dispatch.max_count">500000</s:key>
```

```
<s:key name="dispatch.max_time">0</s:key>
<s:key name="dispatch.reduce_freq">10</s:key>
<s:key name="dispatch.rt_backfill">0</s:key>
<s:key name="dispatch.rt_maximum_span"></s:key>
<s:key name="dispatch.sample_ratio">1</s:key>
<s:key name="dispatch.spawn_process">1</s:key>
<s:key name="dispatch.time_format">%FT%T.%Q%:z</s:key>
<s:key name="dispatch.ttl">2p</s:key>
<s:key name="dispatchAs">owner</s:key>
<!-- display settings elided -->
<s:key name="displayview"></s:key>
<s:key name="durable.backfill_type">auto</s:key>
<s:key name="durable.lag_time">0</s:key>
<s:key name="durable.max_backfill_intervals">0</s:key>
<s:key name="durable.track_time_type"></s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">search</s:key>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">admin</s:key>
    <s:key name="perms"/>
    <s:key name="removable">1</s:key>
    <s:key name="sharing">user</s:key>
  </s:dict>
</s:key>
<s:key name="eai:attributes">
  <s:dict>
    <s:key name="optionalFields">
      <s:list>
        <!-- action settings elided -->
        <s:item>actions</s:item>
        <s:item>alert.digest_mode</s:item>
        <s:item>alert.expires</s:item>
        <s:item>alert.managedBy</s:item>
        <s:item>alert.severity</s:item>
        <s:item>alert.suppress</s:item>
        <s:item>alert.suppress.fields</s:item>
        <s:item>alert.suppress.group_name</s:item>
        <s:item>alert.suppress.period</s:item>
        <s:item>alert.track</s:item>
        <s:item>alert_comparator</s:item>
        <s:item>alert_condition</s:item>
        <s:item>alert_threshold</s:item>
        <s:item>alert_type</s:item>
        <s:item>allow_skew</s:item>
        <s:item>auto_summarize</s:item>
        <s:item>auto_summarize.command</s:item>
        <s:item>auto_summarize.cron_schedule</s:item>
        <s:item>auto_summarize.dispatch.earliest_time</s:item>
        <s:item>auto_summarize.dispatch.latest_time</s:item>
        <s:item>auto_summarize.dispatch.time_format</s:item>
        <s:item>auto_summarize.dispatch.ttl</s:item>
        <s:item>auto_summarize.max_concurrent</s:item>
        <s:item>auto_summarize.max_disabled_buckets</s:item>
        <s:item>auto_summarize.max_summary_ratio</s:item>
        <s:item>auto_summarize.max_summary_size</s:item>
        <s:item>auto_summarize.max_time</s:item>
        <s:item>auto_summarize.suspend_period</s:item>
        <s:item>auto_summarize.timespan</s:item>
        <s:item>auto_summarize.workload_pool</s:item>
        <s:item>cron_schedule</s:item>
        <s:item>defer_scheduled_searchable_idxc</s:item>
        <s:item>description</s:item>
        <s:item>disabled</s:item>
        <s:item>dispatch.allow_partial_results</s:item>
        <s:item>dispatch.auto_cancel</s:item>
        <s:item>dispatch.auto_pause</s:item>
        <s:item>dispatch.buckets</s:item>
        <s:item>dispatch.earliest_time</s:item>
        <s:item>dispatch.index_earliest</s:item>
        <s:item>dispatch.index_latest</s:item>
        <s:item>dispatch.indexedRealtime</s:item>
        <s:item>dispatch.indexedRealtimeMinSpan</s:item>
        <s:item>dispatch.indexedRealtimeOffset</s:item>
        <s:item>dispatch.latest_time</s:item>
        <s:item>dispatch.lookups</s:item>
        <s:item>dispatch.max_count</s:item>
        <s:item>dispatch.max_time</s:item>
        <s:item>dispatch.reduce_freq</s:item>
        <s:item>dispatch.rt_backfill</s:item>
        <s:item>dispatch.rt_maximum_span</s:item>
        <s:item>dispatch.sample_ratio</s:item>
        <s:item>dispatch.spawn_process</s:item>
        <s:item>dispatch.time_format</s:item>
        <s:item>dispatch.ttl</s:item>
        <s:item>dispatchAs</s:item>
        <!-- display settings elided -->
        <s:item>displayview</s:item>
        <s:item>durable.backfill_type</s:item>
        <s:item>durable.lag_time</s:item>
        <s:item>durable.max_backfill_intervals</s:item>
        <s:item>durable.track_time_type</s:item>
        <s:item>estimatedResultCount</s:item>
        <s:item>federated.provider</s:item>
        <s:item>hint</s:item>
        <s:item>is_scheduled</s:item>
        <s:item>is_visible</s:item>
        <s:item>max_concurrent</s:item>
        <s:item>next_scheduled_time</s:item>
        <s:item>numFields</s:item>
        <s:item>qualifiedSearch</s:item>
        <s:item>realtime_schedule</s:item>
        <s:item>request.ui_dispatch_app</s:item>
        <s:item>request.ui_dispatch_view</s:item>
        <s:item>restart_on_searchpeer_add</s:item>
        <s:item>run_n_times</s:item>
        <s:item>run_on_startup</s:item>
        <s:item>schedule_as</s:item>
        <s:item>schedule_priority</s:item>
        <s:item>schedule_window</s:item>
        <s:item>search</s:item>
        <s:item>skip_scheduled_realtime_idxc</s:item>
        <s:item>vsid</s:item>
        <s:item>workload_pool</s:item>
      </s:list>
    </s:key>
    <s:key name="requiredFields">
      <s:list>
```

```
                <s:item>name</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list>
                <s:item>action\..*</s:item>
                <s:item>args\..*</s:item>
                <s:item>dispatch\..*</s:item>
                <s:item>display\.statistics\.format\..*</s:item>
                <s:item>display\.visualizations\.custom\..*</s:item>
                <s:item>durable\..*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="embed.enabled">0</s:key>
        <s:key name="federated.provider"></s:key>
        <s:key name="is_scheduled">0</s:key>
        <s:key name="is_visible">1</s:key>
        <s:key name="max_concurrent">1</s:key>
        <s:key name="next_scheduled_time"></s:key>
        <s:key name="qualifiedSearch">search search index=_internal | stats count by host</s:key>
        <s:key name="realtime_schedule">1</s:key>
        <s:key name="request.ui_dispatch_app"></s:key>
        <s:key name="request.ui_dispatch_view"></s:key>
        <s:key name="restart_on_searchpeer_add">1</s:key>
        <s:key name="run_n_times">0</s:key>
        <s:key name="run_on_startup">0</s:key>
        <s:key name="schedule_as">auto</s:key>
        <s:key name="schedule_priority">default</s:key>
        <s:key name="schedule_window">0</s:key>
        <s:key name="search">search index=_internal | stats count by host</s:key>
        <s:key name="skip_scheduled_realtime_idxc">0</s:key>
        <s:key name="vsid"></s:key>
        <s:key name="workload_pool"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/searches/{name}

`https://<host>:<mPort>/services/saved/searches/{name}`

Manage the `{name}` saved search.

DELETE

Delete the named saved search.

Request parameters

None

Returned values

None

Example request and response

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch
```

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>savedsearch</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
  <updated>2011-07-13T12:09:05-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
  <!-- opensearch nodes elided for brevity. -->
  <s:messages/>
</feed>
```

GET

Access the named saved search.

Request parameters

Name	Type	Default	Description
earliest_time	String		If the search is scheduled display scheduled times starting from this time
latest_time	String		If the search is scheduled display scheduled times ending at this time
listDefaultActionArgs	Boolean		Indicates whether to list default actions.
add_orphan_field	Boolean		Indicates whether the response includes a boolean value for each saved search to show whether the search is orphaned, meaning that it has no valid owner. When *add_orphan_field* is set to `true`, the response includes the orphaned search indicators, either `0` to indicate that a search is not orphaned or `1` to indicate that the search is orphaned. Admins can use this setting to check for searches without valid owners and resolve related issues.

Returned values

Name	Description
action.<action_name>	Indicates whether the `<action_name>` is enabled or disabled for a particular search. For more information about the alert action options see the `alert_actions.conf` file.
action.<action_name>.<parameter>	Overrides the setting defined for an action in the `alert_actions.conf` file with a new setting that is valid only for the search configuration to which it is applied.
action.email	Indicates the state of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart.

Name	Description
	Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.email.format	Specify the format of text in the email. This value also applies to any attachments. Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates.
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. *Note:* This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct a url that can be referenced externally, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost." When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails. Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the global maximum number of search results to send when email.action is enabled.

Name	Description
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.reportServerEnabled	Not supported.
action.email.reportServerURL	Not supported.
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server.
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
action.populate_lookup	The state of the populate lookup action.
action.populate_lookup.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.populate_lookup.hostname	Sets the hostname used in the web link (url) sent in alert actions.

Name	Description
	This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.populate_lookup.maxresults	The maximum number of search results sent using alerts.
action.populate_lookup.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d]
action.populate_lookup.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.populate_lookup.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]
action.rss	The state of the RSS action.
action.rss.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.rss.hostname	Sets the hostname used in the web link (url) sent in alert actions.
action.rss.maxresults	Sets the maximum number of search results sent using alerts.
action.rss.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.
action.rss.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.rss.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.script	The state of the script action.
action.script.command	The search command (or pipeline) which is responsible for executing the action.

Name	Description
	Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.script.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See *action.email.hostname* for details.
action.script.maxresults	The maximum number of search results sent using alerts.
action.script.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted.
action.script.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.script.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.summary_index	The state of the summary index action.
action.summary_index._name	Specifies the name of the summary index where the results of the scheduled search are saved. Defaults to "summary."
action.summary_index._type"	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to `event` or `metric`.
action.summary_index.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.summary_index.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)

Name	Description
	See action.email.hostname for details.
action.summary_index.force_realtime_schedule	By default, *realtime_schedule* is `false` for a report configured for summary indexing. When set to `1` or `true`, this setting overrides *realtime_schedule*. Setting this setting to `true` can cause gaps in summary data, as a *realtime_schedule* search is skipped if search concurrency limits are violated.
action.summary_index.inline	Determines whether to execute the summary indexing action as part of the scheduled search. *Note:* This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).
action.summary_index.maxresults	Sets the maximum number of search results sent using alerts.
action.summary_index.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.
action.summary_index.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.summary_index.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
alert.digest_mode	Specifies whether alert actions are applied to the entire result set or to each individual result.
alert.expires	Sets the period of time to show the alert in the dashboard. Defaults to 24h.
alert.managedBy	Specifies the feature or component that created the alert.
alert.severity	Valid values: (1 | 2 | 3 | 4 | 5 | 6) Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL
alert.suppress	Indicates whether alert suppression is enabled for this schedules search.
alert.suppress.fields	List of fields to use when suppressing per-result alerts. Must be specified if the digest mode is disabled and suppression is enabled.
alert.suppress.group_name	Optional setting. Used to define an alert suppression group for a set of alerts that are running over identical or very similar datasets. Alert suppression groups can help you avoid getting multiple triggered alert notifications for the same data.
alert.suppress.period	Specifies the suppression period. Only valid if alert.suppress is enabled. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.

Name	Description
alert.track	Specifies whether to track the actions triggered by this scheduled search. `auto` - (Default) Determine whether to apply alert tracking to this search, based on the tracking setting of each action. Do not track scheduled searches that always trigger actions. `true` - Force alert tracking for this search. Default. `false` - Disable alert tracking for this search.
alert_comparator	One of the following strings: greater than less than equal to rises by drops by rises by perc drops by perc Used with *alert_threshold* to trigger alert actions.
alert_condition	A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. *Note:* If you specify an *alert_condition*, do not set counttype, relation, or quantity.
alert_threshold	Valid values are: Integer[%] Specifies the value to compare (see *alert_comparator*) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to *rises by perc" or "drops by perc."*
alert_type	What to base the alert on, overridden by *alert_condition* if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources. Typically, reports return the "always" value, while alerts can return any other value.

allow_skew	`0 | <percentage> | <duration>`
	Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.
	Caution: This setting does not require adjusting in most use cases. Check with an admin before making any updates.
	When set to a non-zero value for searches with the following `cron_schedule` values, the search scheduler randomly skews the second, minute, and hour on which the search runs.
	`* * * * *     Every minute.`
	`*/M * * * *   Every M minutes (M > 0).`

Name	Description

	`0 * * * *     Every hour.`
	`0 */H * * *   Every H hours (H > 0).`
	`0 0 * * *     Every day (at midnight).`
	When set to a non-zero value for a search that has any other `cron_schedule` setting, the search scheduler can randomly skew only the second on which the search runs.
	The amount of skew for a specific search remains constant between edits of the search.
	A value of `0` disallows skew. `0` is the default setting.
	Percentage
	`<int>` followed by `%` specifies the maximum amount of time to skew as a percentage of the scheduled search period.
	Duration
	`<int><unit>` specifies a maximum duration. The `<unit>` can be omitted only when the `<int>` is `0`.
	Valid duration units:
	• `m`
	• `min`
	• `minute`
	• `mins`
	• `minutes`
	• `h`
	• `hr`
	• `hour`
	• `hrs`
	• `hours`
	• `d`
	• `day`
	• `days`
	Examples
	`100% (for an every-5-minute search) = 5 minutes maximum`
	`50% (for an every-minute search) = 30 seconds maximum`
	`5m = 5 minutes maximum`
	`1h = 1 hour maximum`

auto_summarize	Specifies whether the search scheduler should ensure that the data for this search is automatically summarized.
auto_summarize.command	A search template to use to construct the auto-summarization for the search. Do not change.
auto_summarize.cron_schedule	Cron schedule to use to probe or generate the summaries for this search
auto_summarize.dispatch.<arg-name>	Dispatch options that can be overridden when running the summary search.
auto_summarize.max_concurrent	The maximum number of concurrent instances of this auto summarizing search that the scheduler is allowed to run.

Name	Description
auto_summarize.max_disabled_buckets	The maximum number of buckets with suspended summarization before the summarization search is completely stopped and the summarization of the search is suspended for the value specified by the *auto_summarize.suspend_period* setting.
auto_summarize.max_summary_ratio	The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket.
auto_summarize.max_summary_size	The minimum summary size, in bytes, before testing whether the summarization is helpful.
auto_summarize.max_time	The maximum time, in seconds, that the auto-summarization search is allowed to run.
auto_summarize.suspend_period	The amount of time to suspend summarization of the search if the summarization is deemed unhelpful.
auto_summarize.timespan	Comma-delimited list of time ranges that each summarized chunk should span. Comprises the list of available summary ranges for which summaries would be available. Does not support `1w` timespans.
auto_summarize.workload_pool	Sets the name of the workload pool that is used by the auto-summarization of this search.
cron_schedule	The cron schedule to run this search. For more information, refer to the description of this parameter in the POST endpoint.
defer_scheduled_searchable_idxc	Specifies whether to defer a continuous saved search during a searchable rolling restart or searchable rolling upgrade of an indexer cluster.
description	Description of this saved search.
disabled	Indicates if this saved search is disabled.
dispatch.allow_partial_results	Specifies whether the search job can proceed to provide partial results if a search peer fails. When set to false, the search job fails if a search peer providing results for the search job fails.
dispatch.auto_cancel	Specifies the amount of inactive time, in seconds, after which the search job is automatically canceled.
dispatch.auto_pause	Specifies the amount of inactive time, in seconds, after which the search job is automatically paused.
dispatch.buckets	The maximum number of timeline buckets.
dispatch.earliest_time	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.index_earliest	Specifies the earliest index time for this search. Can be a relative or absolute time.
dispatch.index_latest	Specifies the latest index time for this saved search. Can be a relative or absolute time.
dispatch.indexedRealtime	Specifies whether to use 'indexed-realtime' mode when doing real-time searches.
dispatch.indexedRealtimeMinSpan	Specifies the minimum number of seconds to wait between component index searches.
dispatch.indexedRealtimeOffset	Specifies the number of seconds to wait for disk flushes to finish.
dispatch.indexedRealtimeMinSpan	Allows for a per-job override of the `[search] indexed_realtime_default_span` setting in `limits.conf`. The default for saved searches is "unset", falling back to the `limits.conf` setting.
dispatch.latest_time	A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.lookups	Indicates if lookups are enabled for this search.
dispatch.max_count	The maximum number of results before finalizing the search.

Name	Description
dispatch.max_time	Indicates the maximum amount of time (in seconds) before finalizing the search.
dispatch.reduce_freq	Specifies how frequently the MapReduce reduce phase runs on accumulated map values.
dispatch.rt_backfill	Specifies whether to do real-time window backfilling for scheduled real-time searches.
dispatch.rt_maximum_span	Sets the maximum number of seconds to search data that falls behind real time.
dispatch.sample_ratio	The integer value used to calculate the sample ratio. The formula is `1 / <integer>`.
dispatch.spawn_process	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Indicates whether a new search process spawns when this saved search is executed.
dispatch.time_format	A time format string that defines the time format for specifying the earliest and latest time.
dispatch.ttl	Indicates the time to live (ttl), in seconds, for the artifacts of the scheduled search, if no actions are triggered.
displayview	Defines the default Splunk Web view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.
durable.backfill_type	Specifies how the Splunk software backfills the lost search results of failed scheduled search jobs. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*. Valid values are `auto`, `time_interval`, and `time_whole`.
durable.lag_time	Specifies the search time delay, in seconds, that a durable search uses to catch events that are ingested or indexed late. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.max_backfill_intervals	Specifies the maximum number of cron intervals (previous scheduled search jobs) that the Splunk software can attempt to backfill for this search, when those jobs have incomplete events. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.track_time_type	Indicates that a scheduled search is durable and specifies how the search tracks events. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
earliest_time	For scheduled searches display all the scheduled times starting from this time.
is_scheduled	Indicates if this search is to be run on a schedule.
is_visible	Indicates if this saved search appears in the visible saved search list.
latest_time	For scheduled searches display all the scheduled times until this time (not just the next run time).
listDefaultActionArgs	List default values of actions.*, even though some of the actions may not be specified in the saved search.
max_concurrent	The maximum number of concurrent instances of this search the scheduler is allowed to run.
next_scheduled_time	The time when the scheduler runs this search again.
orphan	If the `add_orphan_field` parameter is passed in with the GET request, this field indicates whether the search is orphaned.

Name	Description
qualifiedSearch	The exact search command for this saved search.
realtime_schedule	Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. See the POST parameter for this attribute for details.
request.ui_dispatch_app	A field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	Specifies a field used by Splunk Web to denote the view this search should be displayed in.
restart_on_searchpeer_add	Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. *Note:* The peer can be a newly added peer or a peer down and now available.
run_n_times	Runs this search exactly the specified number of times. Does not run the search again until the Splunk platform is restarted.
run_on_startup	Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Set run_on_startup to true for scheduled searches that populate lookup tables.

schedule_priority	Indicates the scheduling priority of a specific search. One of the following values.
	`[ default | higher | highest ]`
	Raises the scheduling priority of the named search.
	default
	No scheduling priority increase.
	higher
	Scheduling priority is higher than other searches of the same scheduling tier. While there are four tiers of priority for scheduled searches, only the following are affected by this property:
	`* real-Time-Scheduled (realtime_schedule=1).`
	`* continuous-Scheduled (realtime_schedule=0).`
	highest
	Scheduling priority is higher than other searches regardless of scheduling tier. However, real-time-scheduled searches with `priority = highest` always have priority over continuous scheduled searches with `priority = highest`.
	The high-to-low priority order (where RTSS = real-time-scheduled search,
	`CSS = continuous-scheduled search, d = default, h = higher, H = highest)`
	`is:`
	`RTSS(H) > CSS(H) > RTSS(h) > RTSS(d) > CSS(h) > CSS(d)`

Name	Description
	Requires the search owner to have the `edit_search_schedule_priority` capability in order to make non-default settings. Defaults to `default`. For more details, see `savedsearches.conf.spec`.
schedule_window	Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to `auto`, the scheduler determines the optimal time window automatically.
search	Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has "foo" as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.
vsid	Defines the viewstate id associated with the UI view listed in 'displayview'. Must match up to a stanza in viewstates.conf.

Example request and response

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://fool01:8092/services/saved/searches</id>
  <updated>2021-04-29T10:00:27-07:00</updated>
  <generator build="84cbec3d51a6" version="8.2.2105"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <link href="/services/saved/searches/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>MySavedSearch</title>
    <id>https://fool01:8092/servicesNS/admin/search/saved/searches/MySavedSearch</id>
    <updated>2021-04-29T09:58:12-07:00</updated>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="list"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/embed" rel="embed"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/history" rel="history"/>
    <content type="text/xml">
      <s:dict>
        < ---- action settings elided  ---- >
        <s:key name="actions"></s:key>
        <s:key name="alert.digest_mode">1</s:key>
        <s:key name="alert.expires">24h</s:key>
        <s:key name="alert.managedBy"></s:key>
        <s:key name="alert.severity">3</s:key>
        <s:key name="alert.suppress"></s:key>
        <s:key name="alert.suppress.fields"></s:key>
        <s:key name="alert.suppress.group_name"></s:key>
        <s:key name="alert.suppress.period"></s:key>
        <s:key name="alert.track">0</s:key>
        <s:key name="alert_comparator"></s:key>
        <s:key name="alert_condition"></s:key>
        <s:key name="alert_threshold"></s:key>
        <s:key name="alert_type">always</s:key>
        <s:key name="allow_skew">0</s:key>
        <s:key name="auto_summarize">0</s:key>
        <s:key name="auto_summarize.command"><![CDATA[| summarize override=partial
timespan=$auto_summarize.timespan$ max_summary_size=$auto_summarize.max_summary_size$
max_summary_ratio=$auto_summarize.max_summary_ratio$
max_disabled_buckets=$auto_summarize.max_disabled_buckets$ max_time=$auto_summarize.max_time$ [ $search$
]]]></s:key>
        <s:key name="auto_summarize.cron_schedule">*/10 * * * *</s:key>
        <s:key name="auto_summarize.dispatch.earliest_time"></s:key>
        <s:key name="auto_summarize.dispatch.latest_time"></s:key>
        <s:key name="auto_summarize.dispatch.time_format">%FT%T.%Q%:z</s:key>
        <s:key name="auto_summarize.dispatch.ttl">60</s:key>
        <s:key name="auto_summarize.max_concurrent">1</s:key>
        <s:key name="auto_summarize.max_disabled_buckets">2</s:key>
        <s:key name="auto_summarize.max_summary_ratio">0.1</s:key>
        <s:key name="auto_summarize.max_summary_size">52428800</s:key>
        <s:key name="auto_summarize.max_time">3600</s:key>
        <s:key name="auto_summarize.suspend_period">24h</s:key>
        <s:key name="auto_summarize.timespan"></s:key>
        <s:key name="auto_summarize.workload_pool"></s:key>
        <s:key name="cron_schedule">*/3 * * * *</s:key>
        <s:key name="defer_scheduled_searchable_idxc">0</s:key>
        <s:key name="description">This test job is a durable saved search</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="dispatch.allow_partial_results">1</s:key>
        <s:key name="dispatch.auto_cancel">0</s:key>
        <s:key name="dispatch.auto_pause">0</s:key>
        <s:key name="dispatch.buckets">0</s:key>
        <s:key name="dispatch.earliest_time">-24h@h</s:key>
        <s:key name="dispatch.index_earliest"></s:key>
        <s:key name="dispatch.index_latest"></s:key>
        <s:key name="dispatch.indexedRealtime"></s:key>
        <s:key name="dispatch.indexedRealtimeMinSpan"></s:key>
        <s:key name="dispatch.indexedRealtimeOffset"></s:key>
        <s:key name="dispatch.latest_time">now</s:key>
        <s:key name="dispatch.lookups">1</s:key>
        <s:key name="dispatch.max_count">500000</s:key>
        <s:key name="dispatch.max_time">0</s:key>
        <s:key name="dispatch.reduce_freq">10</s:key>
        <s:key name="dispatch.rt_backfill">0</s:key>
```

```
<s:key name="dispatch.rt_maximum_span"></s:key>
<s:key name="dispatch.sample_ratio">1</s:key>
<s:key name="dispatch.spawn_process">1</s:key>
<s:key name="dispatch.time_format">%FT%T.%Q%:z</s:key>
<s:key name="dispatch.ttl">2p</s:key>
<s:key name="dispatchAs">owner</s:key>
< ---- display settings elided  ---- >
<s:key name="displayview"></s:key>
<s:key name="durable.backfill_type">time_interval</s:key>
<s:key name="durable.lag_time">30</s:key>
<s:key name="durable.max_backfill_intervals">100</s:key>
<s:key name="durable.track_time_type">_time</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">search</s:key>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">admin</s:key>
    <s:key name="perms"/>
    <s:key name="removable">1</s:key>
    <s:key name="sharing">user</s:key>
  </s:dict>
</s:key>
<s:key name="eai:attributes">
  <s:dict>
    <s:key name="optionalFields">
      <s:list>
        < ---- action settings elided  ---- >
        <s:item>actions</s:item>
        <s:item>alert.digest_mode</s:item>
        <s:item>alert.expires</s:item>
        <s:item>alert.managedBy</s:item>
        <s:item>alert.severity</s:item>
        <s:item>alert.suppress</s:item>
        <s:item>alert.suppress.fields</s:item>
        <s:item>alert.suppress.group_name</s:item>
        <s:item>alert.suppress.period</s:item>
        <s:item>alert.track</s:item>
        <s:item>alert_comparator</s:item>
        <s:item>alert_condition</s:item>
        <s:item>alert_threshold</s:item>
        <s:item>alert_type</s:item>
        <s:item>allow_skew</s:item>
        <s:item>auto_summarize</s:item>
        <s:item>auto_summarize.command</s:item>
        <s:item>auto_summarize.cron_schedule</s:item>
        <s:item>auto_summarize.dispatch.earliest_time</s:item>
        <s:item>auto_summarize.dispatch.latest_time</s:item>
        <s:item>auto_summarize.dispatch.time_format</s:item>
        <s:item>auto_summarize.dispatch.ttl</s:item>
        <s:item>auto_summarize.max_concurrent</s:item>
        <s:item>auto_summarize.max_disabled_buckets</s:item>
        <s:item>auto_summarize.max_summary_ratio</s:item>
        <s:item>auto_summarize.max_summary_size</s:item>
        <s:item>auto_summarize.max_time</s:item>
        <s:item>auto_summarize.suspend_period</s:item>
        <s:item>auto_summarize.timespan</s:item>
        <s:item>auto_summarize.workload_pool</s:item>
        <s:item>cron_schedule</s:item>
        <s:item>defer_scheduled_searchable_idxc</s:item>
        <s:item>description</s:item>
        <s:item>disabled</s:item>
        <s:item>dispatch.allow_partial_results</s:item>
        <s:item>dispatch.auto_cancel</s:item>
        <s:item>dispatch.auto_pause</s:item>
        <s:item>dispatch.buckets</s:item>
        <s:item>dispatch.earliest_time</s:item>
        <s:item>dispatch.index_earliest</s:item>
        <s:item>dispatch.index_latest</s:item>
        <s:item>dispatch.indexedRealtime</s:item>
        <s:item>dispatch.indexedRealtimeMinSpan</s:item>
        <s:item>dispatch.indexedRealtimeOffset</s:item>
        <s:item>dispatch.latest_time</s:item>
        <s:item>dispatch.lookups</s:item>
        <s:item>dispatch.max_count</s:item>
        <s:item>dispatch.max_time</s:item>
        <s:item>dispatch.reduce_freq</s:item>
        <s:item>dispatch.rt_backfill</s:item>
        <s:item>dispatch.rt_maximum_span</s:item>
        <s:item>dispatch.sample_ratio</s:item>
        <s:item>dispatch.spawn_process</s:item>
        <s:item>dispatch.time_format</s:item>
        <s:item>dispatch.ttl</s:item>
        <s:item>dispatchAs</s:item>
        < ---- display settings elided  ---- >
        <s:item>displayview</s:item>
        <s:item>durable.backfill_type</s:item>
        <s:item>durable.lag_time</s:item>
        <s:item>durable.max_backfill_intervals</s:item>
        <s:item>durable.track_time_type</s:item>
        <s:item>estimatedResultCount</s:item>
        <s:item>federated.provider</s:item>
        <s:item>hint</s:item>
        <s:item>is_scheduled</s:item>
        <s:item>is_visible</s:item>
        <s:item>max_concurrent</s:item>
        <s:item>next_scheduled_time</s:item>
        <s:item>numFields</s:item>
        <s:item>qualifiedSearch</s:item>
        <s:item>realtime_schedule</s:item>
        <s:item>request.ui_dispatch_app</s:item>
        <s:item>request.ui_dispatch_view</s:item>
        <s:item>restart_on_searchpeer_add</s:item>
        <s:item>run_n_times</s:item>
        <s:item>run_on_startup</s:item>
        <s:item>schedule_as</s:item>
        <s:item>schedule_priority</s:item>
        <s:item>schedule_window</s:item>
        <s:item>search</s:item>
        <s:item>skip_scheduled_realtime_idxc</s:item>
        <s:item>vsid</s:item>
        <s:item>workload_pool</s:item>
      </s:list>
    </s:key>
    <s:key name="requiredFields">
      <s:list/>
    </s:key>
    <s:key name="wildcardFields">
      <s:list>
```

```
                <s:item>action\..*</s:item>
                <s:item>args\..*</s:item>
                <s:item>dispatch\..*</s:item>
                <s:item>display\.statistics\.format\..*</s:item>
                <s:item>display\.visualizations\.custom\..*</s:item>
                <s:item>durable\..*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="embed.enabled">0</s:key>
        <s:key name="federated.provider"></s:key>
        <s:key name="is_scheduled">0</s:key>
        <s:key name="is_visible">1</s:key>
        <s:key name="max_concurrent">1</s:key>
        <s:key name="next_scheduled_time"></s:key>
        <s:key name="qualifiedSearch">search search index=_internal | stats count by host</s:key>
        <s:key name="realtime_schedule">1</s:key>
        <s:key name="request.ui_dispatch_app"></s:key>
        <s:key name="request.ui_dispatch_view"></s:key>
        <s:key name="restart_on_searchpeer_add">1</s:key>
        <s:key name="run_n_times">0</s:key>
        <s:key name="run_on_startup">0</s:key>
        <s:key name="schedule_as">auto</s:key>
        <s:key name="schedule_priority">default</s:key>
        <s:key name="schedule_window">0</s:key>
        <s:key name="search">search index=_internal | stats count by host</s:key>
        <s:key name="skip_scheduled_realtime_idxc">0</s:key>
        <s:key name="vsid"></s:key>
        <s:key name="workload_pool"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update the named saved search.

Request parameters

Name	Type	Description
action.<action_name>	Boolean	Enable or disable an alert action. See `alert_actions.conf` for available alert action types. `action_name` defaults to the empty string.
action.<action_name>.<parameter>	String or Number	Use this syntax to configure action parameters. See `alert_actions.conf` for parameter options.
action.summary_index._type"	String	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to `event` or `metric`.
action.summary_index.force_realtime_schedule	Boolean	By default, *realtime_schedule* is `false` for a report configured for summary indexing. When set to `1` or `True`, this setting overrides *realtime_schedule*. Setting this setting to `true` can cause gaps in summary data, as a *realtime_schedule* search is skipped if search concurrency limits are violated.
actions	String	A comma-separated list of actions to enable.

Name	Type	Description
		For example: rss,email
alert.digest_mode	Boolean	Specifies whether alert actions are applied to the entire result set or on each individual result. Defaults to 1 (true).
alert.expires	Number	Valid values: [number][time-unit] Sets the period of time to show the alert in the dashboard. Defaults to 24h. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.severity	Enum	Valid values: (1 | 2 | 3 | 4 | 5 | 6) Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL Defaults to 3.
alert.suppress	Boolean	Indicates whether alert suppression is enabled for this scheduled search.
alert.suppress.fields	String	Comma delimited list of fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
alert.suppress.group_name	String	Optional setting. Used to define an alert suppression group for a set of alerts that are running over identical or very similar datasets. Alert suppression groups can help you avoid getting multiple triggered alert notifications for the same data.
alert.suppress.period	Number	Valid values: [number][time-unit] Specifies the suppression period. Only valid if *alert.suppress* is enabled. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.track	Enum	Valid values: (true | false | auto) Specifies whether to track the actions triggered by this scheduled search. `auto` - Determine whether to apply alert tracking to this search, based on the tracking setting of each action. Do not track scheduled searches that always trigger actions. Default. `true` - Force alert tracking for this search. `false` - Disable alert tracking for this search.

Name	Type	Description
alert_comparator	String	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc. Used with *alert_threshold* to trigger alert actions.
alert_condition	String	Contains a conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. **Note:** If you specify an alert_condition, do not set counttype, relation, or quantity.
alert_threshold	Number	Valid values are: Integer[%] Specifies the value to compare (see *alert_comparator*) before triggering the alert actions. If expressed as a percentage, indicates value to use when *alert_comparator* is set to "rises by perc" or "drops by perc."
alert_type	String	What to base the alert on, overridden by *alert_condition* if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.

allow_skew	`0 | <percentage> | <duration>`	Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.
		Caution: This setting does not require adjusting in most use cases. Check with an admin before making any updates.
		When set to a non-zero value for searches with the following *cron_schedule* values, the search scheduler randomly skews the second, minute, and hour on which the search runs.
		`* * * * *     Every minute.`
		`*/M * * * *   Every M minutes (M > 0).`
		`0 * * * *     Every hour.`
		`0 */H * * *   Every H hours (H > 0).`
		`0 0 * * *     Every day (at midnight).`
		When set to a non-zero value for a search that has any other `cron_schedule` setting, the search scheduler can randomly skew only the second on which the search runs.
		The amount of skew for a specific search remains constant between edits of the search.
		A value of `0` disallows skew. `0` is the default setting.

Name	Type	Description

		Percentage
		`<int>` followed by `%` specifies the maximum amount of time to skew as a percentage of the scheduled search period.
		Duration
		`<int><unit>` specifies a maximum duration. The `<unit>` can be omitted only when the `<int>` is `0`.
		Valid duration units:
		• `m`
		• `min`
		• `minute`
		• `mins`
		• `minutes`
		• `h`
		• `hr`
		• `hour`
		• `hrs`
		• `hours`
		• `d`
		• `day`
		• `days`
		Examples
		`100% (for an every-5-minute search) = 5 minutes maximum`
		`50% (for an every-minute search) = 30 seconds maximum`
		`5m = 5 minutes maximum`
		`1h = 1 hour maximum`

*args.**	String	Wildcard argument that accepts any saved search template argument, such as args.username=foobar when the search is search $username$.
auto_summarize	Boolean	Indicates whether the scheduler should ensure that the data for this search is automatically summarized. Defaults to 0.
auto_summarize.command	String	An auto summarization template for this search. See auto summarization options in `savedsearches.conf` for more details. Do not change unless you understand the architecture of saved search auto summarization.
auto_summarize.cron_schedule	String	Cron schedule that probes and generates the summaries for this saved search. The default value is `*/10 * * * *` and corresponds to "every ten hours".
auto_summarize.dispatch.earliest_time	String	A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.

Name	Type	Description
auto_summarize.dispatch.latest_time	String	A time string that specifies the latest time for summarizing this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
auto_summarize.dispatch.time_format	String	Defines the time format that Splunk software uses to specify the earliest and latest time. Defaults to `%FT%T.%Q%:z`
auto_summarize.dispatch.ttl	String	Valid values: Integer[p]. Indicates the time to live (ttl), in seconds, for the artifacts of the summarization of the scheduled search. Defaults to 60.
auto_summarize.max_disabled_buckets	Number	The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for auto_summarize.suspend_period. Defaults to 2.
auto_summarize.max_summary_ratio	Number	The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. Defaults to `0.1` *Note:* The test is only performed if the summary size is larger than auto_summarize.max_summary_size.
auto_summarize.max_summary_size	Number	The minimum summary size, in bytes, before testing whether the summarization is helpful. The default value is `52428800` and is equivalent to 5MB.
auto_summarize.max_time	Number	Maximum time (in seconds) that the summary search is allowed to run. Defaults to 3600. *Note:* This is an approximate time. The summary search stops at clean bucket boundaries.
auto_summarize.suspend_period	String	Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful. Defaults to 24h.
auto_summarize.timespan	String	Comma-delimited list of time ranges that each summarized chunk should span. Comprises the list of available granularity levels for which summaries would be available. Does not support `1w` timespans. For example, a timechart over the last month whose granularity is at the day level should set this to `1d`. If you need the same data summarized at the hour level for weekly charts, use: `1h,1d`.
cron_schedule	String	Valid values: cron string The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this

Name	Type	Description
		type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.
description	String	Human-readable description of this saved search. Defaults to empty string.
disabled	Boolean	Indicates if the saved search is enabled. Defaults to 0. Disabled saved searches are not visible in Splunk Web.
*dispatch.**	String	Wildcard argument that accepts any dispatch related argument.
dispatch.allow_partial_results	Boolean	Specifies whether the search job can proceed to provide partial results if a search peer fails. When set to false, the search job fails if a search peer providing results for the search job fails.
dispatch.auto_cancel	Number	Specifies the amount of inactive time, in seconds, after which the search job is automatically canceled.
dispatch.auto_pause	Number	Specifies the amount of inactive time, in seconds, after which the search job is automatically paused.
dispatch.buckets	Number	The maximum number of timeline buckets. Defaults to 0.
dispatch.earliest_time	String	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.index_earliest	String	A time string that specifies the earliest index time for this search. Can be a relative or absolute time.
dispatch.index_latest	String	A time string that specifies the latest index time for this saved search. Can be a relative or absolute time.
dispatch.indexedRealtime	Boolean	Indicates whether to used indexed-realtime mode when doing real-time searches.
dispatch.indexedRealtimeOffset	Integer	Allows for a per-job override of the `[search] indexed_realtime_disk_sync_delay` setting in `limits.conf`. Default for saved searches is "unset", falling back to `limits.conf` setting.
dispatch.indexedRealtimeMinSpan	Integer	Allows for a per-job override of the `[search] indexed_realtime_default_span` setting in `limits.conf`. Default for saved searches is "unset", falling back to the `limits.conf` setting.
dispatch.latest_time	String	

Name	Type	Description
		A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the *dispatch.time_format* to format the value.
dispatch.lookups	Boolean	Enables or disables the lookups for this search. Defaults to 1.
dispatch.max_count	Number	The maximum number of results before finalizing the search. Defaults to 500000.
dispatch.max_time	Number	Indicates the maximum amount of time (in seconds) before finalizing the search. Defaults to 0.
dispatch.reduce_freq	Number	Specifies, in seconds, how frequently the MapReduce reduce phase runs on accumulated map values. Defaults to 10.
dispatch.rt_backfill	Boolean	Whether to back fill the real time window for this search. Parameter valid only if this is a real time search. Defaults to 0.
dispatch.rt_maximum_span	Number	Allows for a per-job override of the `[search] indexed_realtime_maximum_span` setting in `limits.conf`. Default for saved searches is "unset", falling back to the `limits.conf` setting.
dispatch.sample_ratio	Number	The integer value used to calculate the sample ratio. The formula is `1 / <integer>`.
dispatch.spawn_process	Boolean	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Specifies whether a new search process spawns when this saved search is executed. Defaults to 1. Searches against indexes *must* run in a separate process.
dispatch.time_format	String	A time format string that defines the time format for specifying the earliest and latest time. Defaults to `%FT%T.%Q%:z`
dispatch.ttl	Number	Valid values: Integer[p]. Defaults to 2p. Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered. If an action is triggered, the ttl changes to that action ttl. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to `alert_actions.conf.spec`. If the integer is followed by the letter 'p', the ttl is handled as a multiple of the scheduled search period.
dispatchAs	String	When the saved search is dispatched using the "saved/searches/{name}/dispatch" endpoint, this setting controls what user that search is dispatched as. Only meaningful for shared saved searches. Can be set to `owner` or `user`.
displayview	String	Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.

Name	Type	Description
durable.backfill_type	String	Specifies how the Splunk software backfills the lost search results of failed scheduled search jobs. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*. Valid values are `auto`, `time_interval`, and `time_whole`. `time_whole` - The Splunk software schedules a single backfill search job with a time range that spans the combined time ranges of all failed scheduled search jobs. The `time_whole` setting can be applied only to searches that are streaming, where the results are raw events without additional aggregation. `time_interval` - The Splunk software schedules multiple backfill search jobs, one for each failed scheduled search job. The backfill jobs have time ranges that match those of the failed jobs. The `time_interval` setting can be applied to both streaming and non-streaming searches. `auto` - The Splunk software decides the backfill type by checking whether the search is streaming or not. If the search is streaming, the Splunk software uses the `time_whole` backfill type. Otherwise, it uses the `time_interval` backfill type.
durable.lag_time	Number	Specifies the search time delay, in seconds, that a durable search uses to catch events that are ingested or indexed late. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.max_backfill_intervals	Number	Specifies the maximum number of cron intervals (previous scheduled search jobs) that the Splunk software can attempt to backfill for this search, when those jobs have incomplete events. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.track_time_type	String	Indicates that a scheduled search is durable and specifies how the search tracks events. A durable search is a search that tries to ensure the delivery of all results, even when the search process is slowed or stopped by runtime issues like rolling restarts, network bottlenecks, and even downed servers. Applies only to scheduled searches. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
is_scheduled	Boolean	Whether this search is to be run on a schedule
is_visible	Boolean	Specifies whether this saved search should be listed in the visible saved search list. Defaults to 1.

Name	Type	Description
max_concurrent	Number	The maximum number of concurrent instances of this search the scheduler is allowed to run. Defaults to 1.
next_scheduled_time	String	Read-only attribute. Value ignored on POST. There are some old clients who still send this value
qualifiedSearch	String	Read-only attribute. Value ignored on POST. The value is computed during runtime.
realtime_schedule	Boolean	Defaults to 1. Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).
request.ui_dispatch_app	String	Specifies a field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	String	Specifies a field used by Splunk Web to denote the view this search should be displayed in.
restart_on_searchpeer_add	Boolean	Specifies whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. Defaults to 1. **Note:** The peer can be a newly added peer or a peer down and now available.
run_n_times	Number	Runs this search exactly the specified number of times. Does not run the search again until the Splunk platform is restarted.
run_on_startup	Boolean	Indicates whether this search runs at startup. If it does not run on startup, it runs at the next scheduled time. Defaults to 0. Set to 1 for scheduled searches that populate lookup tables.
schedule_window	Number or `auto`	Time window (in minutes) during which the search has lower priority. Defaults to 0. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period.

Name	Type	Description
		Set to `auto` to let the scheduler determine the optimal window value automatically. Requires the `edit_search_schedule_window` capability to override `auto`.
search	String	**Required.** The search to save.
schedule_priority	See description	Raises the scheduling priority of the named search. Use one of the following options. default No scheduling priority increase. higher Scheduling priority is higher than other searches of the same scheduling tier. While there are four tiers of priority for scheduled searches, only the following search types are affected by this property. real-time scheduled (realtime_schedule=1). continuous scheduled (realtime_schedule=0). highest Scheduling priority is higher than other searches regardless of scheduling tier. However, real-time-scheduled searches with `priority = highest` always have priority over continuous scheduled searches with `priority = highest`. Requires the search owner to have the `edit_search_schedule_priority` capability in order to make non-default settings. Defaults to `default`. For more details, see `savedsearches.conf.spec`.
vsid	String	Defines the viewstate id associated with the UI view listed in 'displayview'. Must match up to a stanza in viewstates.conf.
workload_pool	String	Specifies the new workload pool where the existing running search will be placed.

Returned values

Name	Description
action.<action_name>	Indicates whether the `<action_name>` is enabled or disabled for a particular search. For more information about the alert action options see the `alert_actions.conf` file.
action.<action_name>.<parameter>	Overrides the setting defined for an action in the `alert_actions.conf` file with a new setting that is valid only for the search configuration to which it is applied.
action.email	Indicates the state of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the next restart. Defaults to empty string.

Name	Description
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.email.format	Specify the format of text in the email. This value also applies to any attachments.< Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates. Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf.
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct a url that can be referenced externally, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails. Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the global maximum number of search results to send when email.action is enabled.

Name	Description
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.pdfview	The name of the view to deliver if sendpdf is enabled
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportCIDFontList	Space-separated list. Specifies the set (and load order) of CID fonts for handling Simplified Chinese(gb), Traditional Chinese(cns), Japanese(jp), and Korean(kor) in Integrated PDF Rendering. If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used. To skip loading any CID fonts, specify the empty string. Default value: "gb cns jp kor"
action.email.reportIncludeSplunkLogo	Indicates whether to include the Splunk logo with the report.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.reportServerEnabled	Not supported.
action.email.reportServerURL	Not supported.
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server.
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).

Name	Description
action.email.width_sort_columns	Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.
action.populate_lookup	Indicates the state of the populate lookup action.
action.populate_lookup.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.populate_lookup.dest	Lookup name of path of the lookup to populate.
action.populate_lookup.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.populate_lookup.maxresults	The maximum number of search results sent using alerts.
action.populate_lookup.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d]
action.populate_lookup.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.populate_lookup.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]
action.rss	Indicates the state of the RSS action.
action.rss.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.rss.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms:

Name	Description
	hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.rss.maxresults	Sets the maximum number of search results sent using alerts.
action.rss.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Valid values are Integer[m |s |h |d].
action.rss.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.rss.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
action.script	Indicates the state of the script for this action.
action.script.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.script.filename	File name of the script to call. Required if script action is enabled
action.script.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.script.maxresults	Sets the maximum number of search results sent using alerts.
action.script.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted.
action.script.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.script.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.

Name	Description
	Valid values are: Integer[p]
action.summary_index	Indicates the state of the summary index.
action.summary_index._name	Specifies the name of the summary index where the results of the scheduled search are saved. Defaults to "summary."
action.summary_index.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.summary_index.hostname	Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) See action.email.hostname for details.
action.summary_index.inline	Determines whether to execute the summary indexing action as part of the scheduled search. *Note:* This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).
action.summary_index.maxresults	Sets the maximum number of search results sent using alerts.
action.summary_index.maxtime	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d]
action.summary_index.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.summary_index.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]
actions	Actions triggerd by this alert.
alert.digest_mode	Indicates if the alert actions are applied to the entire result set or to each individual result.
alert.expires	Sets the period of time to show the alert in the dashboard. Defaults to 24h. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.

Name	Description
	Valid values: [number][time-unit]
alert.severity	Valid values: (1 | 2 | 3 | 4 | 5 | 6) Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL
alert.suppress	Indicates whether alert suppression is enabled for this schedules search.
alert.suppress.fields	Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
alert.suppress.period	Specifies the suppresion period. Only valid if alert.supress is enabled. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.track	Specifies whether to track the actions triggered by this scheduled search. auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions. true - force alert tracking. false - disable alert tracking for this search.
alert_comparator	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc
alert_condition	A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. *Note:* If you specify an alert_condition, do not set counttype, relation, or quantity.
alert_threshold	Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to "rises by perc" or "drops by perc."
alert_type	What to base the alert on, overriden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
allow_skew	`0 | <percentage> | <duration>` Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.

Name	Description

	Caution: This setting does not require adjusting in most use cases. Check with an admin before making any updates.
	When set to a non-zero value for searches with the following `cron_schedule` values, the search scheduler randomly skews the second, minute, and hour on which the search runs.
	`* * * * *     Every minute.`
	`*/M * * * *   Every M minutes (M > 0).`
	`0 * * * *     Every hour.`
	`0 */H * * *   Every H hours (H > 0).`
	`0 0 * * *     Every day (at midnight).`
	When set to a non-zero value for a search that has any other `cron_schedule` setting, the search scheduler can randomly skew only the second on which the search runs.
	The amount of skew for a specific search remains constant between edits of the search.
	A value of `0` disallows skew. `0` is the default setting.
	Percentage
	`<int>` followed by `%` specifies the maximum amount of time to skew as a percentage of the scheduled search period.
	Duration
	`<int><unit>` specifies a maximum duration. The `<unit>` can be omitted only when the `<int>` is `0` (which disables skew).
	Valid duration units:
	• `m`
	• `min`
	• `minute`
	• `mins`
	• `minutes`
	• `h`
	• `hr`
	• `hour`
	• `hrs`
	• `hours`
	• `d`
	• `day`
	• `days`
	Examples
	`100% (for an every-5-minute search) = 5 minutes maximum`
	`50% (for an every-minute search) = 30 seconds maximum`
	`5m = 5 minutes maximum`
	`1h = 1 hour maximum`

Name	Description
*args.**	Wildcard argument that accepts any saved search template argument, such as args.username=foobar when the search is search $username$.
auto_summarize	Indicates whether the scheduler should ensure that the data for this search is automatically summarized.
auto_summarize.command	A search template that constructs the auto summarization for this search. **Caution:** Advanced feature. Do not change unless you understand the architecture of auto summarization of saved searches.
auto_summarize.cron_schedule	Cron schedule that probes and generates the summaries for this saved search.
auto_summarize.dispatch.earliest_time	A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time.
auto_summarize.dispatch.latest_time	A time string that specifies the latest time for this saved search. Can be a relative or absolute time.
auto_summarize.dispatch.time_format	Time format used to specify the earliest and latest times.
auto_summarize.dispatch.ttl	Indicates the time to live (in seconds) for the artifacts of the summarization of the scheduled search. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.
auto_summarize.max_disabled_buckets	The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for auto_summarize.suspend_period.
auto_summarize.max_summary_ratio	The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. *Note:* The test is only performed if the summary size is larger than auto_summarize.max_summary_size.
auto_summarize.max_summary_size	The minimum summary size, in bytes, before testing whether the summarization is helpful.
auto_summarize.max_time	Maximum time (in seconds) that the summary search is allowed to run. *Note:* This is an approximate time. The summary search stops at clean bucket boundaries.
auto_summarize.suspend_period	Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful.
auto_summarize.timespan	The list of time ranges that each summarized chunk should span. This comprises the list of available granularity levels for which summaries would be available. For example a timechart over the last month whose granularity is at the day level should set this to 1d. If you need the same data summarized at the hour level for weekly charts, use: 1h,1d.
cron_schedule	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43.

Name	Description
	Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string
description	Description of this saved search. Defaults to empty string.
disabled	Indicates if this saved search is disabled.
*dispatch.**	* represents any custom dispatch field.
dispatch.buckets	The maximum nuber of timeline buckets.
dispatch.earliest_time	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
dispatch.indexedRealtime	Indicates whether to used indexed-realtime mode when doing real-time searches.
dispatch.latest_time	A time string that specifies the latest time for the saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
dispatch.lookups	Indicates if lookups are enabled for this search.
dispatch.max_count	The maximum number of results before finalizing the search.
dispatch.max_time	Indicates the maximum amount of time (in seconds) before finalizing the search.
dispatch.reduce_freq	Specifies how frequently the MapReduce reduce phase runs on accumulated map values.
dispatch.rt_backfill	Indicates whether to back fill the real time window for this search. Parameter valid only if this is a real time search
dispatch.spawn_process	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Indicates whether a new search process spawns when this saved search is executed.
dispatch.time_format	Time format string that defines the time format for specifying the earliest and latest time.
dispatch.ttl	Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered. If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to `alert_actions.conf.spec`. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.
displayview	Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.
durable.backfill_type	Specifies how the Splunk software backfills the lost search results of failed scheduled search jobs. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*. Valid values are `auto`, `time_interval`, and `time_whole`.

Name	Description
durable.lag_time	Specifies the search time delay, in seconds, that a durable search uses to catch events that are ingested or indexed late. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.max_backfill_intervals	Specifies the maximum number of cron intervals (previous scheduled search jobs) that the Splunk software can attempt to backfill for this search, when those jobs have incomplete events. Applies only to scheduled searches that have a valid setting other than `none` for *durable.track_time_type*.
durable.track_time_type	Indicates that a scheduled search is durable and specifies how the search tracks events. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
is_scheduled	Indicates if this search is to be run on a schedule.
is_visible	Indicates if this saved search appears in the visible saved search list.
max_concurrent	The maximum number of concurrent instances of this search the scheduler is allowed to run.
next_scheduled_time	The time when the scheduler runs this search again.
qualifiedSearch	The exact search string that the scheduler would run.
realtime_schedule	Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).
request.ui_dispatch_app	A field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	Specifies a field used by Splunk Web to denote the view this search should be displayed in.
restart_on_searchpeer_add	Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. *Note:* The peer can be a newly added peer or a peer down and now available.
run_on_startup	Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Splunk recommends that you set run_on_startup to true for scheduled searches that populate lookup tables.
schedule_window	Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to `auto`, the scheduler prioritizes searches automatically.
search	

Name	Description
	Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has "foo" as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.
vsid	The viewstate id associated with the UI view listed in 'displayview'. Matches to a stanza in viewstates.conf.

Example request and response

```
curl -k -u admin:chang2me https://fool01:8092/services/saved/searches/test_durable  -d
durable.track_time_type=_time -d durable.max_backfill_intervals=100  -d durable.lag_time=30 -d
durable.backfill_type=time_interval
```

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://fool01:8092/services/saved/searches</id>
  <updated>2021-04-29T09:58:12-07:00</updated>
  <generator build="84cbec3d51a6" version="8.2.2105"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <link href="/services/saved/searches/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>test_durable</title>
    <id>https://fool01:8092/servicesNS/admin/search/saved/searches/test_durable</id>
    <updated>2021-04-29T09:58:12-07:00</updated>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="list"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/embed" rel="embed"/>
    <link href="/servicesNS/admin/search/saved/searches/test_durable/history" rel="history"/>
    <content type="text/xml">
      <s:dict>
        <!-- action settings elided -->
        <s:key name="actions"></s:key>
        <s:key name="alert.digest_mode">1</s:key>
        <s:key name="alert.expires">24h</s:key>
        <s:key name="alert.managedBy"></s:key>
        <s:key name="alert.severity">3</s:key>
        <s:key name="alert.suppress"></s:key>
        <s:key name="alert.suppress.fields"></s:key>
        <s:key name="alert.suppress.group_name"></s:key>
        <s:key name="alert.suppress.period"></s:key>
        <s:key name="alert.track">0</s:key>
        <s:key name="alert_comparator"></s:key>
        <s:key name="alert_condition"></s:key>
        <s:key name="alert_threshold"></s:key>
        <s:key name="alert_type">always</s:key>
        <s:key name="allow_skew">0</s:key>
        <s:key name="auto_summarize">0</s:key>
        <s:key name="auto_summarize.command"><![CDATA[| summarize override=partial
timespan=$auto_summarize.timespan$ max_summary_size=$auto_summarize.max_summary_size$
max_summary_ratio=$auto_summarize.max_summary_ratio$
max_disabled_buckets=$auto_summarize.max_disabled_buckets$ max_time=$auto_summarize.max_time$ [ $search$
]]]></s:key>
        <s:key name="auto_summarize.cron_schedule">*/10 * * * *</s:key>
        <s:key name="auto_summarize.dispatch.earliest_time"></s:key>
        <s:key name="auto_summarize.dispatch.latest_time"></s:key>
        <s:key name="auto_summarize.dispatch.time_format">%FT%T.%Q%:z</s:key>
        <s:key name="auto_summarize.dispatch.ttl">60</s:key>
        <s:key name="auto_summarize.max_concurrent">1</s:key>
        <s:key name="auto_summarize.max_disabled_buckets">2</s:key>
        <s:key name="auto_summarize.max_summary_ratio">0.1</s:key>
        <s:key name="auto_summarize.max_summary_size">52428800</s:key>
        <s:key name="auto_summarize.max_time">3600</s:key>
        <s:key name="auto_summarize.suspend_period">24h</s:key>
        <s:key name="auto_summarize.timespan"></s:key>
        <s:key name="auto_summarize.workload_pool"></s:key>
        <s:key name="cron_schedule">*/3 * * * *</s:key>
        <s:key name="defer_scheduled_searchable_idxc">0</s:key>
        <s:key name="description">This test job is a durable saved search</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="dispatch.allow_partial_results">1</s:key>
        <s:key name="dispatch.auto_cancel">0</s:key>
        <s:key name="dispatch.auto_pause">0</s:key>
        <s:key name="dispatch.buckets">0</s:key>
        <s:key name="dispatch.earliest_time">-24h@h</s:key>
        <s:key name="dispatch.index_earliest"></s:key>
        <s:key name="dispatch.index_latest"></s:key>
        <s:key name="dispatch.indexedRealtime"></s:key>
        <s:key name="dispatch.indexedRealtimeMinSpan"></s:key>
        <s:key name="dispatch.indexedRealtimeOffset"></s:key>
        <s:key name="dispatch.latest_time">now</s:key>
        <s:key name="dispatch.lookups">1</s:key>
        <s:key name="dispatch.max_count">500000</s:key>
        <s:key name="dispatch.max_time">0</s:key>
        <s:key name="dispatch.reduce_freq">10</s:key>
        <s:key name="dispatch.rt_backfill">0</s:key>
        <s:key name="dispatch.rt_maximum_span"></s:key>
        <s:key name="dispatch.sample_ratio">1</s:key>
        <s:key name="dispatch.spawn_process">1</s:key>
        <s:key name="dispatch.time_format">%FT%T.%Q%:z</s:key>
        <s:key name="dispatch.ttl">2p</s:key>
        <s:key name="dispatchAs">owner</s:key>
        <!-- display settings elided -->
        <s:key name="displayview"></s:key>
        <s:key name="durable.backfill_type">time_interval</s:key>
        <s:key name="durable.lag_time">30</s:key>
        <s:key name="durable.max_backfill_intervals">100</s:key>
```

```
<s:key name="durable.track_time_type">_time</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">search</s:key>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">admin</s:key>
    <s:key name="perms"/>
    <s:key name="removable">1</s:key>
    <s:key name="sharing">user</s:key>
  </s:dict>
</s:key>
<s:key name="eai:attributes">
  <s:dict>
    <s:key name="optionalFields">
      <s:list>
        <!-- action settings elided -->
        <s:item>actions</s:item>
        <s:item>alert.digest_mode</s:item>
        <s:item>alert.expires</s:item>
        <s:item>alert.managedBy</s:item>
        <s:item>alert.severity</s:item>
        <s:item>alert.suppress</s:item>
        <s:item>alert.suppress.fields</s:item>
        <s:item>alert.suppress.group_name</s:item>
        <s:item>alert.suppress.period</s:item>
        <s:item>alert.track</s:item>
        <s:item>alert_comparator</s:item>
        <s:item>alert_condition</s:item>
        <s:item>alert_threshold</s:item>
        <s:item>alert_type</s:item>
        <s:item>allow_skew</s:item>
        <s:item>auto_summarize</s:item>
        <s:item>auto_summarize.command</s:item>
        <s:item>auto_summarize.cron_schedule</s:item>
        <s:item>auto_summarize.dispatch.earliest_time</s:item>
        <s:item>auto_summarize.dispatch.latest_time</s:item>
        <s:item>auto_summarize.dispatch.time_format</s:item>
        <s:item>auto_summarize.dispatch.ttl</s:item>
        <s:item>auto_summarize.max_concurrent</s:item>
        <s:item>auto_summarize.max_disabled_buckets</s:item>
        <s:item>auto_summarize.max_summary_ratio</s:item>
        <s:item>auto_summarize.max_summary_size</s:item>
        <s:item>auto_summarize.max_time</s:item>
        <s:item>auto_summarize.suspend_period</s:item>
        <s:item>auto_summarize.timespan</s:item>
        <s:item>auto_summarize.workload_pool</s:item>
        <s:item>cron_schedule</s:item>
        <s:item>defer_scheduled_searchable_idxc</s:item>
        <s:item>description</s:item>
        <s:item>disabled</s:item>
        <s:item>dispatch.allow_partial_results</s:item>
        <s:item>dispatch.auto_cancel</s:item>
        <s:item>dispatch.auto_pause</s:item>
        <s:item>dispatch.buckets</s:item>
        <s:item>dispatch.earliest_time</s:item>
        <s:item>dispatch.index_earliest</s:item>
        <s:item>dispatch.index_latest</s:item>
        <s:item>dispatch.indexedRealtime</s:item>
        <s:item>dispatch.indexedRealtimeMinSpan</s:item>
        <s:item>dispatch.indexedRealtimeOffset</s:item>
        <s:item>dispatch.latest_time</s:item>
        <s:item>dispatch.lookups</s:item>
        <s:item>dispatch.max_count</s:item>
        <s:item>dispatch.max_time</s:item>
        <s:item>dispatch.reduce_freq</s:item>
        <s:item>dispatch.rt_backfill</s:item>
        <s:item>dispatch.rt_maximum_span</s:item>
        <s:item>dispatch.sample_ratio</s:item>
        <s:item>dispatch.spawn_process</s:item>
        <s:item>dispatch.time_format</s:item>
        <s:item>dispatch.ttl</s:item>
        <s:item>dispatchAs</s:item>
        <!-- display settings elided -->
        <s:item>displayview</s:item>
        <s:item>durable.backfill_type</s:item>
        <s:item>durable.lag_time</s:item>
        <s:item>durable.max_backfill_intervals</s:item>
        <s:item>durable.track_time_type</s:item>
        <s:item>estimatedResultCount</s:item>
        <s:item>federated.provider</s:item>
        <s:item>hint</s:item>
        <s:item>is_scheduled</s:item>
        <s:item>is_visible</s:item>
        <s:item>max_concurrent</s:item>
        <s:item>next_scheduled_time</s:item>
        <s:item>numFields</s:item>
        <s:item>qualifiedSearch</s:item>
        <s:item>realtime_schedule</s:item>
        <s:item>request.ui_dispatch_app</s:item>
        <s:item>request.ui_dispatch_view</s:item>
        <s:item>restart_on_searchpeer_add</s:item>
        <s:item>run_n_times</s:item>
        <s:item>run_on_startup</s:item>
        <s:item>schedule_as</s:item>
        <s:item>schedule_priority</s:item>
        <s:item>schedule_window</s:item>
        <s:item>search</s:item>
        <s:item>skip_scheduled_realtime_idxc</s:item>
        <s:item>vsid</s:item>
        <s:item>workload_pool</s:item>
      </s:list>
    </s:key>
    <s:key name="requiredFields">
      <s:list/>
    </s:key>
    <s:key name="wildcardFields">
      <s:list>
        <s:item>action\..*</s:item>
        <s:item>args\..*</s:item>
        <s:item>dispatch\..*</s:item>
        <s:item>display\.statistics\.format\..*</s:item>
        <s:item>display\.visualizations\.custom\..*</s:item>
        <s:item>durable\..*</s:item>
      </s:list>
    </s:key>
  </s:dict>
</s:key>
<s:key name="embed.enabled">0</s:key>
```

```
        <s:key name="federated.provider"></s:key>
        <s:key name="is_scheduled">0</s:key>
        <s:key name="is_visible">1</s:key>
        <s:key name="max_concurrent">1</s:key>
        <s:key name="next_scheduled_time"></s:key>
        <s:key name="qualifiedSearch">search search index=_internal | stats count by host</s:key>
        <s:key name="realtime_schedule">1</s:key>
        <s:key name="request.ui_dispatch_app"></s:key>
        <s:key name="request.ui_dispatch_view"></s:key>
        <s:key name="restart_on_searchpeer_add">1</s:key>
        <s:key name="run_n_times">0</s:key>
        <s:key name="run_on_startup">0</s:key>
        <s:key name="schedule_as">auto</s:key>
        <s:key name="schedule_priority">default</s:key>
        <s:key name="schedule_window">0</s:key>
        <s:key name="search">search index=_internal | stats count by host</s:key>
        <s:key name="skip_scheduled_realtime_idxc">0</s:key>
        <s:key name="vsid"></s:key>
        <s:key name="workload_pool"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/searches/{name}/acknowledge

`https://<host>:<mPort>/services/saved/searches/{name}/acknowledge`

Acknowledge the `{name}` saved search alert suppression.

POST

Acknowledge the `{name}` saved search alert suppression and resume alerting.

Request parameters

Name	Type	Default	Description
key	String		The suppression key used in field-based suppression. For example, in host-based suppression, with data from 5 hosts, the key is the host, as each host could have different suppression expiration times.

Returned values

None

Example request and response

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MyAlert/acknowledge -X
POST
```

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
  <updated>2011-07-26T18:31:07-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

saved/searches/{name}/dispatch

`https://<host>:<mPort>/services/saved/searches/{name}/dispatch`

Dispatch the `{name}` saved search.

POST

Dispatch the `{name}` saved search.

Request parameters

Name	Type	Default	Description
*args.**			Arg values to create a saved search is the saved search is a template search. For example, specify arg.index_name to create the following search: search index=$args.index_name$ | ...
dispatchAs	String	"owner" | "user"	Indicate the user context, quota, and access rights for the saved search. The saved search runs according to the context indicated.
*dispatch.**	String		Any dispatch.* field of the search that needs to be overridden when running the summary search.
dispatch.adhoc_search_level	String		Use one of the following search modes. `[verbose	fast	smart]`
dispatch.now	Boolean		Dispatch the search as if the specified time for this parameter was the current time.
force_dispatch	Boolean		Indicates whether to start a new search even if another instance of this search is already running.
now	String		[Deprecated] Use *dispatch.now*.
replay_speed	Number greater than 0		Indicate a real-time search replay speed factor. For example, `1` indicates normal speed. `0.5` indicates half of normal speed, and `2` indicates twice as fast as normal.

Name	Type	Default	Description

			`earliest_time` and `latest_time` arguments must indicate a real-time time range to use replay options.
			Use *replay_speed* with *replay_et* and *replay_lt* relative times to indicate a speed and time range for the replay. For example,
			`replay_speed = 10`
			`replay_et = -d@d`
			`replay_lt = -@d`
			specifies a replay at 10x speed, as if the "wall clock" time starts yesterday at midnight and ends when it reaches today at midnight.
			For more information about using relative time modifiers, see Search time modifiers in the *Search reference*.

replay_et	Time modifier string		Relative "wall clock" start time for the replay.
replay_lt	Time modifier string.		Relative end time for the replay clock. The replay stops when clock time reaches this time.
trigger_actions	Boolean		Indicates whether to trigger alert actions.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch/dispatch
-d trigger_actions=1
```

XML Response

```
<?xml version='1.0' encoding='UTF-8'?>
<response><sid>admin__admin__search__MySavedSearch_at_1311797437_d831d980832e3e89</sid></response>
```

saved/searches/{name}/history

`https://<host>:<mPort>/services/saved/searches/{name}/history`

List available search jobs created from the `{name}` saved search.

GET

List available search jobs created from the `{name}` saved search.

Request parameters

Name	Description
savedsearch	String triplet consisting of `user:app:search_name`. The triplet constitutes a unique identifier for accessing saved search history. Passing in this parameter can help you work around saved search access limitations in search head clustered deployments. As an example, the following parameter triplet represents an `admin` user, the `search` app context, and a search named `Splunk errors last 24 hours`. `savedsearch=admin:search:Splunk%20errors%20last%2024%20hours`

Returned values

Name	Description
durableTrackTime	The durable cursor **timestamp** for the search job, expressed in UNIX Epoch time notation (elapsed time since 1/1/1970). If `durableTrackType=_indextime`, this timestamp is associated with the indexed timestamp of the events returned by the job. If `durableTrackType=_time`, this timestamp is associated with the event timestamp of the events returned by the job.
durableTrackType	Indicates that a scheduled search is durable and specifies how the search tracks events. A value of `_time` means the durable search tracks each event by its event **timestamp** , based on time information included in the event. A value of `_indextime` means the durable search tracks each event by its indexed timestamp. The search is not durable if this setting is unset or is set to `none`.
earliest_time	The earliest time a search job is configured to start.
isDone	Indicates if the search has completed.
isFinalized	Indicates if the search was finalized (stopped before completion).
isRealTimeSearch	Indicates if the search is a real time search.
isSaved	Indicates if the search is saved indefinitely.
isScheduled	Indicates if the search is a scheduled search.
isZombie	Indicates if the process running the search is dead, but with the search not finished.
latest_time	The latest time a search job is configured to start.
listDefaultActionArgs	List default values of actions.*, even though some of the actions may not be specified in the saved search.
ttl	The time to live, or time before the search job expires after it completes.

Example request and response

XML Request

```
curl -k -u admin:pass https://fool01:8092/services/saved/searches/summary_durable/history
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>summary_durable</title>
  <id>https://fool01:8092/services/saved/searches</id>
  <updated>2021-04-29T10:01:20-07:00</updated>
  <generator build="84cbec3d51a6" version="8.2.2105"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_acl" rel="_acl"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler__admin__search__RMD50dbc462560ef18a2_at_1619715420_1</title>
    <id>https://fool01:8092/servicesNS/nobody/search/search/jobs/scheduler__admin__search_
_RMD50dbc462560ef18a2_at_1619715420_1</id>
    <updated>2021-04-29T09:57:44-07:00</updated>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search__RMD50dbc462560ef18a2_at_1619715420_1"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <published>2021-04-29T09:57:17-07:00</published>
    <content type="text/xml">
      <s:dict>
        <s:key name="durableTrackTime">1619715420.000000000</s:key>
        <s:key name="durableTrackType">_time</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="isDone">1</s:key>
        <s:key name="isFinalized">0</s:key>
        <s:key name="isRealTimeSearch">0</s:key>
        <s:key name="isSaved">0</s:key>
        <s:key name="isScheduled">1</s:key>
        <s:key name="isZombie">0</s:key>
        <s:key name="start">1619715437</s:key>
        <s:key name="ttl">118</s:key>
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>scheduler__admin__search__RMD50dbc462560ef18a2_at_1619715600_3</title>
    <id>https://fool01:8092/servicesNS/nobody/search/search/jobs/scheduler__admin__search_
_RMD50dbc462560ef18a2_at_1619715600_3</id>
    <updated>2021-04-29T10:00:14-07:00</updated>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search__RMD50dbc462560ef18a2_at_1619715600_3"
rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <published>2021-04-29T10:00:00-07:00</published>
    <content type="text/xml">
      <s:dict>
        <s:key name="durableTrackTime">1619715600.000000000</s:key>
        <s:key name="durableTrackType">_time</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">admin</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="isDone">1</s:key>
        <s:key name="isFinalized">0</s:key>
        <s:key name="isRealTimeSearch">0</s:key>
        <s:key name="isSaved">0</s:key>
        <s:key name="isScheduled">1</s:key>
        <s:key name="isZombie">0</s:key>
        <s:key name="start">1619715600</s:key>
        <s:key name="ttl">281</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/searches/{name}/reschedule

`https://<host>:<mPort>/services/saved/searches/{name}/reschedule`

Set `{name}` scheduled saved search to start at a specific time and then run on its schedule thereafter.

POST

Define a new start time for a scheduled saved search.

Usage details

If no `schedule_time` argument is specified, the Splunk software runs the search as soon as possible according to its saved search definition. If you restart your Splunk platform implementation, all `schedule_time` values for searches are removed.

Request parameters

Name	Type	Default	Description
schedule_time	Timestamp		The next time to run the search. The timestamp can be in one of three formats: ISO8601 format (adjusted for UTC time), UNIX time format, or relative time format.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/saved/searches/Purchased%20products%2C%20last%2024%20hours/reschedule -d
schedule_time=schedule_time=2018-08-15T14:11:01-08:00
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://localhost:8089/services/saved/searches</id>
  <updated>2018-08-15T14:11:01-08:00</updated>
  <generator build="131547" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

saved/searches/{name}/scheduled_times

`https://<host>:<mPort>/services/saved/searches/{name}/scheduled_times`

Get the `{name}` saved search scheduled time.

GET

Access `{name}` saved search scheduled time.

Request parameters

Name	Type	Default	Description
earliest_time required	String		Absolute or relative earliest time
latest_time required	String		Absolute or relative latest time

Returned values

Name	Description
action.email	Indicates the state of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next platform restart. Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.pdfview	The name of the view to deliver if sendpdf is enabled.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.summary_index	The state of the summary index action.
action.summary_index._name	Specifies the name of the summary index where the results of the scheduled search are saved. Defaults to "summary."
actions	Actions triggered by this alert.
alert.digest_mode	Indicates if alert actions are applied to the entire result set or to each individual result.
alert.expires	Sets the period of time to show the alert in the dashboard. Defaults to 24h. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.severity	Valid values: (1 | 2 | 3 | 4 | 5 | 6)

Name	Description
	Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL
alert.suppress	Indicates whether alert suppression is enabled for this schedules search.
alert.suppress.fields	Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
alert.suppress.period	Specifies the suppression period. Only valid if `alert.supress` is enabled. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
alert.track	Specifies whether to track the actions triggered by this scheduled search. auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions. true - force alert tracking. false - disable alert tracking for this search.
alert_comparator	Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to "rises by perc" or "drops by perc."
alert_condition	A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. *Note:* If you specify an alert_condition, do not set counttype, relation, or quantity.
alert_threshold	Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to "rises by perc" or "drops by perc."
alert_type	What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
cron_schedule	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43.

Name	Description
	Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string
description	Description of the saved search.
disabled	Indicates if this saved search is disabled.
dispatch.buckets	The maximum number of timeline buckets.
dispatch.earliest_time	A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
dispatch.latest_time	A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
dispatch.lookups	Indicates if lookups are enabled for this search.
dispatch.max_count	The maximum number of results before finalizing the search.
dispatch.max_time	Indicates the maximum amount of time (in seconds) before finalizing the search
earliest_time	For scheduled searches display all the scheduled times starting from this time.
is_scheduled	Indicates if this search is to be run on a schedule.
is_visible	Indicates if this saved search appears in the visible saved search list.
latest_time	A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
listDefaultActionArgs	List default values of actions.*, even though some of the actions may not be specified in the saved search.
max_concurrent	The maximum number of concurrent instances of this search the scheduler is allowed to run.
next_scheduled_time	The time when the scheduler runs this search again.
qualifiedSearch	The exact search command for this saved search.
realtime_schedule	Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).

Name	Description
request.ui_dispatch_app	A field used by Splunk Web to denote the app this search should be dispatched in.
request.ui_dispatch_view	A field used by Splunk Web to denote the app this search should be dispatched in.
restart_on_searchpeer_add	Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. *Note:* The peer can be a newly added peer or a peer down and now available.
run_on_startup	Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Splunk recommends that you set run_on_startup to true for scheduled searches that populate lookup tables.
scheduled_times	The times when the scheduler runs the search.
search	Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has "foo" as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.
vsid	The viewstate id associated with the Splunk Web view listed in 'displayview'. Matches to a stanza in viewstates.conf.

Application usage

Specify a time range for the data returned using earliest_time and latest_time parameters.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/services/saved/searches/_ScheduledView__dashboard_live/scheduled_times --get -d
earliest_time=-5h -d latest_time=-3h
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://localhost:8089/services/saved/searches</id>
  <updated>2011-12-02T11:12:55-08:00</updated>
  <generator version="108769"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__dashboard_live</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/searches/_ScheduledView__dashboard_live</id>
    <updated>2011-12-02T11:12:55-08:00</updated>
    <link href="/servicesNS/admin/search/saved/searches/_ScheduledView__dashboard_live" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <!-- opensearch nodes elided for brevity. -->
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.auth_password">$1$o2rN8S6m+0YB</s:key>
        <s:key name="action.email.auth_username">myusername</s:key>
        . . . elided . . .
        <s:key name="action.email.pdfview">dashboard_live</s:key>
        . . . elided . . .
        <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
        <s:key name="action.email.to">myusername@example.com</s:key>
        . . . elided . . .
         <s:key name="action.summary_index">0</s:key>
        <s:key name="action.summary_index._name">summary</s:key>
        . . . elided . . .
        <s:key name="actions">email</s:key>
        <s:key name="alert.digest_mode">1</s:key>
        <s:key name="alert.expires">24h</s:key>
        <s:key name="alert.severity">3</s:key>
        <s:key name="alert.suppress"></s:key>
        <s:key name="alert.suppress.fields"></s:key>
        <s:key name="alert.suppress.period"></s:key>
        <s:key name="alert.track">auto</s:key>
        <s:key name="alert_comparator"></s:key>
        <s:key name="alert_condition"></s:key>
        <s:key name="alert_threshold"></s:key>
        <s:key name="alert_type">always</s:key>
        <s:key name="cron_schedule">*/30 * * * *</s:key>
        <s:key name="description">scheduled search for view name=dashboard_live</s:key>
        <s:key name="disabled">0</s:key>
        <s:key name="dispatch.buckets">0</s:key>
        <s:key name="dispatch.earliest_time">1</s:key>
        <s:key name="dispatch.latest_time">2</s:key>
        <s:key name="dispatch.lookups">1</s:key>
        <s:key name="dispatch.max_count">500000</s:key>
        <s:key name="dispatch.max_time">0</s:key>
        . . . elided . . .
        <!-- eai:acl elided -->
        <s:key name="is_scheduled">1</s:key>
        <s:key name="is_visible">0</s:key>
        <s:key name="max_concurrent">1</s:key>
        <s:key name="next_scheduled_time">2011-12-02 11:30:00 PST</s:key>
        <s:key name="qualifiedSearch"> noop</s:key>
        <s:key name="realtime_schedule">1</s:key>
        <s:key name="request.ui_dispatch_app"></s:key>
        <s:key name="request.ui_dispatch_view"></s:key>
        <s:key name="restart_on_searchpeer_add">1</s:key>
        <s:key name="run_on_startup">0</s:key>
        <s:key name="scheduled_times"><s:list><s:item>1322836200</s:item><s:item>1322838000<
/s:item><s:item>1322839800</s:item><s:item>1322841600</s:item></s:list></s:key>
        <s:key name="search">| noop</s:key>
        <s:key name="vsid"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

saved/searches/{name}/suppress

`https://<host>:<mPort>/services/saved/searches/{name}/suppress`

Get the `{name}` saved search alert suppression state.

GET

Get the `{name}` saved search alert suppression state.

Request parameters

Name	Type	Default	Description
expiration	String		Indicates the time the suppression period expires.
key			

Returned values

Name	Description
earliest_time	For scheduled searches display all the scheduled times starting from this time.
expiration	Sets the period of time to show the alert in the dashboard. Defaults to 24h. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
latest_time	A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.
listDefaultActionArgs	List default values of actions.*, even though some of the actions may not be specified in the saved search.
suppressed	Indicates if alert suppression is enabled for this search.
suppressionKey	A combination of all the values of the suppression fields (or the combinations MD5), if fields were specified.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch/suppress
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>savedsearch</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
  <updated>2011-07-26T18:22:51-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>MySavedSearch</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch</id>
    <updated>2011-07-26T18:22:51-04:00</updated>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="list"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <!-- eai:acl elided -->
        <s:key name="expiration">13811</s:key>
        <s:key name="suppressed">1</s:key>
        <s:key name="suppressionKey">admin;search;MySavedSearch;;</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

scheduled/views

`https://<host>:<mPort>/services/scheduled/views`

Access views scheduled for PDF delivery. Scheduled views are dummy `noop` scheduled saved searches that email a PDF of a dashboard.

GET

List all scheduled view objects.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
action.email	Indicates the state of the email action.
action.email.pdfview	Name of the view to send as a PDF.
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether the search results are included in the email. The results can be attached or inline.
action.email.to	List of recipient email addresses. Required if the email alert action is enabled.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours).

Name	Description
	If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
cron_schedule	The cron schedule to use for delivering the view. Scheduled views are dummy/noop scheduled saved searches that email a pdf version of a view For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.
description	Description of this scheduled view object.
disabled	Indicates if the scheduled view is disabled.
is_scheduled	Indicates if PDF delivery of this view is scheduled.
next_scheduled_time	The next time when the view is delivered.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/scheduled/views
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/admin/scheduledviews</id>
  <updated>2011-07-27T16:27:55-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/admin/scheduledviews/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__MyView</title>
    <id>https://localhost:8089/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView</id>
    <updated>2011-07-27T16:27:55-04:00</updated>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView" rel="list"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/_reload"
rel="_reload"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView" rel="edit"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView" rel="remove"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/move" rel="move"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/disable"
rel="disable"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/dispatch"
rel="dispatch"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/history"
rel="history"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/notify" rel="notify"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.pdfview">MyView</s:key>
        <s:key name="action.email.sendpdf">1</s:key>
        <s:key name="action.email.sendresults"></s:key>
        <s:key name="action.email.to">email@example.com</s:key>
        <s:key name="action.email.ttl">10</s:key>
        <s:key name="cron_schedule">* * * * *</s:key>
        <s:key name="description">scheduled search for view name=MyView</s:key>
        <s:key name="disabled">0</s:key>
        <!-- eai:acl elided -->
        <s:key name="is_scheduled">1</s:key>
        <s:key name="next_scheduled_time">2011-07-27 16:28:00 EDT</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

scheduled/views/{name}

`https://<host>:<mPort>/services/scheduled/views/{name}`

Manage the `{name}` scheduled view.

DELETE

Delete a scheduled view.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
```

```
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/admin/scheduledviews</id>
  <updated>2011-07-27T16:16:02-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/admin/scheduledviews/_reload" rel="_reload"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

GET

Access a scheduled view.

Request parameters
None

Returned values

Name	Description
action.email	Indicates the sate of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the next restart. Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	"BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.email.format	Specify the format of text in the email. This value also applies to any attachments.< Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates. Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf.
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms:

Name	Description
	hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct a url that can be externally referenced, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails. Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the global maximum number of search results to send when email.action is enabled.
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.pdfview	The name of the view to deliver if sendpdf is enabled.
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies the email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	

Name	Description
	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
cron_schedule	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string
description	Description of this saved search for this view.
disabled	Indicates if the saved search for this view is disabled.
is_scheduled	Indicates if this search is to be run on a schedule.
next_scheduled_time	The next time when the view is delivered.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/scheduled/views</id>
  <updated>2011-07-27T17:12:11-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__MyView</title>
    <id>https://localhost:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView</id>
    <updated>2011-07-27T17:12:11-04:00</updated>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="list"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="edit"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="remove"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/move" rel="move"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/history" rel="history"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/notify" rel="notify"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.auth_password"></s:key>
        <s:key name="action.email.auth_username"></s:key>
        <s:key name="action.email.bcc"></s:key>
        <s:key name="action.email.cc"></s:key>
        <s:key name="action.email.command">
          <![CDATA[$action.email.preprocess_results{default=""}$ |
                   sendemail "server=$action.email.mailserver{default=localhost}$"
"use_ssl=$action.email.use_ssl{default=false}$"
                   "use_tls=$action.email.use_tls{default=false}$" "to=$action.email.to$"
"cc=$action.email.cc$"
                   "bcc=$action.email.bcc$" "from=$action.email.from{default=splunk@localhost}$"
                   "subject=$action.email.subject{recurse=yes}$"
"format=$action.email.format{default=csv}$"
                   "sssummary=Saved Search [$name$]: $counttype$($results.count$)" "sslink=$results.url$"
                   "ssquery=$search$" "ssname=$name$" "inline=$action.email.inline{default=False}$"
                   "sendresults=$action.email.sendresults{default=False}$"
"sendpdf=$action.email.sendpdf{default=False}$"
                   "pdfview=$action.email.pdfview$" "searchid=$search_id$"
"graceful=$graceful{default=True}$"
                   maxinputs="$action.email.maxresults{default=10000}$"
maxtime="$action.email.maxtime{default=5m}$"]]>
        </s:key>
        <s:key name="action.email.format">html</s:key>
        <s:key name="action.email.from">splunk</s:key>
        <s:key name="action.email.hostname"></s:key>
        <s:key name="action.email.inline">0</s:key>
        <s:key name="action.email.mailserver">localhost</s:key>
        <s:key name="action.email.maxresults">10000</s:key>
        <s:key name="action.email.maxtime">5m</s:key>
        <s:key name="action.email.pdfview">MyView</s:key>
        <s:key name="action.email.preprocess_results"></s:key>
        <s:key name="action.email.reportPaperOrientation">portrait</s:key>
        <s:key name="action.email.reportPaperSize">letter</s:key>
        <s:key name="action.email.reportServerEnabled">0</s:key>
        <s:key name="action.email.reportServerURL"></s:key>
        <s:key name="action.email.sendpdf">1</s:key>
        <s:key name="action.email.sendresults">0</s:key>
        <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
        <s:key name="action.email.to">info@example.com</s:key>
        <s:key name="action.email.track_alert">1</s:key>
        <s:key name="action.email.ttl">10</s:key>
        <s:key name="action.email.use_ssl">0</s:key>
        <s:key name="action.email.use_tls">0</s:key>
        <s:key name="cron_schedule">* * * * *</s:key>
        <s:key name="description">scheduled search for view name=MyView</s:key>
        <s:key name="disabled">0</s:key>
        <!-- eai:acl elided -->
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>description</s:item>
                <s:item>disabled</s:item>
                <s:item>next_scheduled_time</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>action.email.to</s:item>
                <s:item>cron_schedule</s:item>
                <s:item>is_scheduled</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list><s:item>action\.email.*</s:item></s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="is_scheduled">1</s:key>
        <s:key name="next_scheduled_time">2011-07-27 17:13:00 EDT</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Update a scheduled view.

Request parameters

Name	Type	Default	Description
action.email.to required	String		Comma or semicolon separated list of email addresses to send the view to
*action.email**	String		Wildcard argument that accepts any email action.
cron_schedule required	String		The cron schedule to use for delivering the view. Scheduled views are dummy/noop scheduled saved searches that email a pdf version of a view. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20)

Name	Type	Default	Description
			means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.
description	String		User readable description of this scheduled view object
disabled	Boolean	0	Whether this object is enabled or disabled
is_scheduled required	Boolean		Whether this pdf delivery should be scheduled
next_scheduled_time	String		The next time when the view is delivered. Ignored on edit, here only for backwards compatability.

Returned values

Name	Description
action.email	Indicates the status of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart. Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.email.format	Specify the format of text in the email. This value also applies to any attachments.< Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. NOTE: This means the correct

Name	Description
	port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails. Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the maximum number of search results sent using alerts.
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.pdfview	The name of the view to deliver if sendpdf is enabled.
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server.
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).

Name	Description
cron_schedule	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string
description	Description of the saved search for this view.
disabled	Indicates if the saved search for this view is disabled.
is_scheduled	Indicates if this search is to be run on a schedule.
next_scheduled_time	The next time when the view is delivered.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyVew -d
action.email.to="info@example.com" -d cron_schedule="0 * * * *" -d is_scheduled=1 -d description="New
description"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/scheduled/views</id>
  <updated>2011-07-27T17:59:32-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__MyView</title>
    <id>https://localhost:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView</id>
    <updated>2011-07-27T17:59:32-04:00</updated>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="list"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="edit"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="remove"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/move" rel="move"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/history" rel="history"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/notify" rel="notify"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.auth_password"></s:key>
        <s:key name="action.email.auth_username"></s:key>
        <s:key name="action.email.bcc"></s:key>
        <s:key name="action.email.cc"></s:key>
        <s:key name="action.email.command">
          <![CDATA[$action.email.preprocess_results{default=""}$ |
                   sendemail "server=$action.email.mailserver{default=localhost}$"
"use_ssl=$action.email.use_ssl{default=false}$"
                   "use_tls=$action.email.use_tls{default=false}$" "to=$action.email.to$"
"cc=$action.email.cc$"
                   "bcc=$action.email.bcc$" "from=$action.email.from{default=splunk@localhost}$"
                   "subject=$action.email.subject{recurse=yes}$"
"format=$action.email.format{default=csv}$"
                   "sssummary=Saved Search [$name$]: $counttype$($results.count$)" "sslink=$results.url$"
                   "ssquery=$search$" "ssname=$name$" "inline=$action.email.inline{default=False}$"
                   "sendresults=$action.email.sendresults{default=False}$"
"sendpdf=$action.email.sendpdf{default=False}$"
                   "pdfview=$action.email.pdfview$" "searchid=$search_id$"
"graceful=$graceful{default=True}$"
                   maxinputs="$action.email.maxresults{default=10000}$"
maxtime="$action.email.maxtime{default=5m}$"]]>
        </s:key>
        <s:key name="action.email.format">html</s:key>
        <s:key name="action.email.from">splunk</s:key>
        <s:key name="action.email.hostname"></s:key>
        <s:key name="action.email.inline">0</s:key>
        <s:key name="action.email.mailserver">localhost</s:key>
        <s:key name="action.email.maxresults">10000</s:key>
        <s:key name="action.email.maxtime">5m</s:key>
        <s:key name="action.email.pdfview">MyView</s:key>
        <s:key name="action.email.preprocess_results"></s:key>
        <s:key name="action.email.reportPaperOrientation">portrait</s:key>
        <s:key name="action.email.reportPaperSize">letter</s:key>
        <s:key name="action.email.reportServerEnabled">0</s:key>
        <s:key name="action.email.reportServerURL"></s:key>
        <s:key name="action.email.sendpdf">1</s:key>
        <s:key name="action.email.sendresults">0</s:key>
        <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
        <s:key name="action.email.to">info@example.com</s:key>
        <s:key name="action.email.track_alert">1</s:key>
        <s:key name="action.email.ttl">10</s:key>
        <s:key name="action.email.use_ssl">0</s:key>
        <s:key name="action.email.use_tls">0</s:key>
        <s:key name="cron_schedule">0 * * * *</s:key>
        <s:key name="description">New Description</s:key>
        <s:key name="disabled">0</s:key>
        <!-- eai:acl elided -->
        <s:key name="is_scheduled">1</s:key>
        <s:key name="next_scheduled_time">2011-07-27 18:00:00 EDT</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

scheduled/views/{name}/dispatch

`https://<host>:<mPort>/services/scheduled/views/{name}/dispatch`

Dispatch the scheduled search associated with the `{name}` scheduled view.

POST

Dispatch the scheduled search associated with the `{name}` scheduled view.

Request parameters

Name	Type	Default	Description
*args.**	String		Wildcard argument that accepts any saved search template argument, such as arg.username=foobar when the search is search $username$.
*dispatch.**	String		Wildcard argument that accepts any dispatch related argument.
dispatch.now	Boolean		Dispatch the search as if the specified time for this parameter was the current time.
force_dispatch	Boolean		Indicates whether to start a new search even if another instance of this search is already running.
now	String		[Deprecated] Use *dispatch.now*.
trigger_actions	Boolean		Indicates whether to trigger alert actions

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView/dispatch -d
trigger_actions=1
```

XML Response

```
<?xml version='1.0' encoding='UTF-8'?>
<response><sid>admin__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311805021_c24ff1ea77ad714b</sid><
/response>
```

scheduled/views/{name}/history

`https://<host>:<mPort>/services/scheduled/views/{name}/history`

List search jobs used to render the `{name}` scheduled view.

GET

List search jobs used to render the `{name}` scheduled view.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyVew/history
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>_ScheduledView__MyView</title>
  <id>https://localhost:8089/servicesNS/admin/search/scheduled/views</id>
  <updated>2011-07-27T16:25:22-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a</title>
    <id>https://localhost:8089/servicesNS/nobody/search/search/jobs/scheduler__admin__search
_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a</id>
    <updated>2011-07-27T16:25:15-04:00</updated>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300
_842d7ca298ab521a" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <published>2011-07-27T16:25:15-04:00</published>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300
_842d7ca298ab521a" rel="list"/>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300
_842d7ca298ab521a/_reload" rel="_reload"/>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300
_842d7ca298ab521a" rel="edit"/>
    <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300
_842d7ca298ab521a" rel="remove"/>
    <content type="text/xml">
```

```
      <s:dict>
        <!-- eai:acl elided -->
      </s:dict>
    </content>
  </entry>
</feed>
```

scheduled/views/{name}/reschedule

```
https://<host>:<mPort>/services/scheduled/views/{name}/reschedule
```

Schedule the {name} view PDF delivery.

POST

Schedule the {name} view PDF delivery.

Request parameters

Name	Type	Default	Description
schedule_time	String		Absolute or relative schedule time.

Returned values

None

Application usage

If schedule_time is not specified, then it is assumed that the delivery should occur as soon as possible.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/scheduled/views/_ScheduledView__dashboard2/reschedule
-d schedule_time=2013-02-15T14:11:01Z
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://localhost:8089/services/scheduled/views</id>
  <updated>2012-10-02T08:48:18-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

```
</feed>
```

scheduled/views/{name}/scheduled_times

`https://<host>:<mPort>/services/scheduled/views/{name}/scheduled_times`

Get scheduled view times.

GET

Get scheduled view times.

Request parameters

Name	Type	Default	Description
earliest_time	String		Absolute or relative earliest time
latest_time	String		Absolute or relative latest time

Returned values

Name	Description
action.email	Indicates the state of the email action.
action.email.auth_password	The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart. Defaults to empty string.
action.email.auth_username	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. *Note:* Your SMTP server might reject unauthenticated emails.
action.email.bcc	BCC email address to use if action.email is enabled.
action.email.cc	CC email address to use if action.email is enabled.
action.email.command	The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.
action.email.format	Specify the format of text in the email. This value also applies to any attachments.< Valid values: (plain | html | raw | csv)
action.email.from	Email address from which the email action originates.
action.email.hostname	Sets the hostname used in the web link (url) sent in email actions.

Name	Description
	This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct a url that can be externally referenced, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.
action.email.inline	Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.
action.email.mailserver	Set the address of the MTA server to be used to send the emails. Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).
action.email.maxresults	Sets the maximum number of search results sent using alerts.
action.email.maxtime	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
action.email.pdfview	The name of the view to deliver if sendpdf is enabled.
action.email.preprocess_results	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.
action.email.reportPaperOrientation	Specifies the paper orientation: portrait or landscape.
action.email.reportPaperSize	Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)
action.email.reportServerEnabled	Not supported.
action.email.reportServerURL	Not supported.
action.email.sendpdf	Indicates whether to create and send the results as a PDF.
action.email.sendresults	Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.
action.email.subject	Specifies an email subject. Defaults to SplunkAlert-<savedsearchname>.

Name	Description
action.email.to	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
action.email.track_alert	Indicates whether the execution of this action signifies a trackable alert.
action.email.ttl	Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].
action.email.use_ssl	Indicates whether to use SSL when communicating with the SMTP server.
action.email.use_tls	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
action.email.width_sort_columns	Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.
cron_schedule	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string
description	Description of the saved search for this view.
disabled	Indicates if the saved search for this view is disabled. Disabled saved searches are not visible in Splunk Web.
is_scheduled	Indicates if this search is to be run on a schedule.
next_scheduled_time	The next time when the view is delivered.

Application usage

Specify a time range for the data returned using earliest_time and latest_time parameters.

Example request and response

XML Request

```
curl -k -u admin:admin
https://localhost:8089/services/scheduled/views/_ScheduledView__dashboard_live/scheduled_times --get -d
earliest_time=-5h -d latest_time=-3h
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://wma-mbp15:8089/services/scheduled/views</id>
  <updated>2011-12-01T14:40:18-08:00</updated>
  <generator version="112383"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__dashboard_live</title>
    <id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
    <updated>2011-12-01T14:40:18-08:00</updated>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <!-- opensearch nodes elided for brevity. -->
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.auth_password"></s:key>
        <s:key name="action.email.auth_username"></s:key>
        <s:key name="action.email.bcc"></s:key>
        <s:key name="action.email.cc"></s:key>
        <s:key name="action.email.command"><![CDATA[$action.email.preprocess_results{default=""}$ |
sendemail "server=$action.email.mailserver{default=localhost}$"
"use_ssl=$action.email.use_ssl{default=false}$" "use_tls=$action.email.use_tls{default=false}$"
"to=$action.email.to$" "cc=$action.email.cc$" "bcc=$action.email.bcc$"
"from=$action.email.from{default=splunk@localhost}$" "subject=$action.email.subject{recurse=yes}$"
"format=$action.email.format{default=csv}$" "sssummary=Saved Search [$name$]: $counttype$($results.count$)"
"sslink=$results.url$" "ssquery=$search$" "ssname=$name$" "inline=$action.email.inline{default=False}$"
"sendresults=$action.email.sendresults{default=False}$" "sendpdf=$action.email.sendpdf{default=False}$"
"pdfview=$action.email.pdfview$" "searchid=$search_id$"
"width_sort_columns=$action.email.width_sort_columns$" "graceful=$graceful{default=True}$"
maxinputs="$action.email.maxresults{default=10000}$"
maxtime="$action.email.maxtime{default=5m}$"]]></s:key>
        <s:key name="action.email.format">html</s:key>
        <s:key name="action.email.from">splunk</s:key>
        <s:key name="action.email.hostname"></s:key>
        <s:key name="action.email.inline">0</s:key>
        <s:key name="action.email.mailserver">localhost</s:key>
        <s:key name="action.email.maxresults">10000</s:key>
        <s:key name="action.email.maxtime">5m</s:key>
        <s:key name="action.email.pdfview">dashboard_live</s:key>
        <s:key name="action.email.preprocess_results"></s:key>
        <s:key name="action.email.reportPaperOrientation">portrait</s:key>
        <s:key name="action.email.reportPaperSize">letter</s:key>
        <s:key name="action.email.reportServerEnabled">1</s:key>
        <s:key name="action.email.reportServerURL"> </s:key>
        <s:key name="action.email.sendpdf">1</s:key>
        <s:key name="action.email.sendresults">0</s:key>
        <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
        <s:key name="action.email.to">wma@splunk.com</s:key>
        <s:key name="action.email.track_alert">1</s:key>
        <s:key name="action.email.ttl">10</s:key>
        <s:key name="action.email.use_ssl">0</s:key>
        <s:key name="action.email.use_tls">0</s:key>
        <s:key name="action.email.width_sort_columns">1</s:key>
        <s:key name="cron_schedule">/5 * * * *</s:key>
        <s:key name="description">scheduled search for view name=dashboard_live</s:key>
        <s:key name="disabled">0</s:key>
        <!-- eai:acl elided -->
        <s:key name="is_scheduled">1</s:key>
        <s:key name="next_scheduled_time">2011-12-01 15:00:00 PST</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/concurrency-settings

```
https://<host>:<mPort>/services/search/concurrency-settings
```

GET

List search concurrency settings.

Request parameters

None

Returned values

Name	Type	Description
max_searches_perc	Number	The maximum number of searches the scheduler can run as a percentage of the maximum number of concurrent searches. Default: 50%.
auto_summary_perc	Number	The maximum number of concurrent searches to be allocated for auto summarization, as a percentage of the concurrent searches that the scheduler can run. Default: 50.
max_searches_per_cpu	Number	The maximum number of concurrent historical searches allowed per cpu. Default: 1.
base_max_searches	Number	A baseline constant to add to the max number of searches (computed as multiplier of the CPUs.) Default is 6.
max_rt_search_multiplier	Number	A number by which the maximum number of historical searches is multiplied to determine the maximum number of concurrent real-time searches. Note: The maximum number of real-time searches is computed as max_rt_searches = max_rt_search_multiplier x max_hist_searches

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/concurrency-settings
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
```

```
<title>search-concurrency-settings-handler</title>
<id>https://localhost:8089/services/search/concurrency-settings</id>
<updated>2019-04-21T14:46:39-07:00</updated>
<generator build="efdccca30d13" version="7.3.0"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>scheduler</title>
  <id>https://localhost:8089/services/search/concurrency-settings/scheduler</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/search/concurrency-settings/scheduler" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/concurrency-settings/scheduler" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="auto_summary_perc">50</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list/>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="max_searches_perc">50</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>search</title>
  <id>https://localhost:8089/services/search/concurrency-settings/search</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/search/concurrency-settings/search" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/concurrency-settings/search" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="base_max_searches">10</s:key>
```

```
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="max_rt_search_multiplier">1</s:key>
        <s:key name="max_searches_per_cpu">1</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/concurrency-settings/scheduler

`https://<host>:<mPort>/services/search/concurrency-settings/scheduler`
Edit settings that determine concurrent scheduled search limits.

Authentication and Authorization

The `edit_search_concurrency_scheduled` capability is required for this endpoint.

POST

Edit settings that determine concurrent scheduled search limits.

Request parameters

Name	Type	Description
max_searches_perc	Number	The maximum number of searches the scheduler can run as a percentage of the maximum number of concurrent searches. Default: 50.
auto_summary_perc	Number	The maximum number of concurrent searches to be allocated for auto summarization, as a percentage of the concurrent searches that the scheduler can run. Default: 50.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/concurrency-settings/scheduler -d
max_searches_perc=40
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>search-concurrency-settings-handler</title>
  <id>https://localhost:8089/services/search/concurrency-settings</id>
  <updated>2019-04-21T17:17:30-07:00</updated>
  <generator build="efdccca30d13" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler</title>
    <id>https://localhost:8089/services/search/concurrency-settings/scheduler</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/search/concurrency-settings/scheduler" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/concurrency-settings/scheduler" rel="list"/>
    <link href="/services/search/concurrency-settings/scheduler" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="auto_summary_perc">50</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="max_searches_perc">40</s:key>
    </s:dict>
  </content>
 </entry>
</feed>
```

search/concurrency-settings/search

`https://<host>:<mPort>/services/search/concurrency-settings/search`

Edit settings that determine the maximum number of concurrent scheduled searches.

Authentication and Authorization

The `edit_search_concurrency_all` capability is required for this endpoint.

POST

Edit settings that determine the maximum number of concurrent scheduled searches.

Request parameters

Name	Type	Description
max_searches_per_cpu	Number	The maximum number of concurrent historical searches allowed per cpu. Default: 1.
base_max_searches	Number	A baseline constant to add to the max number of searches (computed as multiplier of the CPUs.) Default is 6.
max_rt_search_multiplier	Number	A number by which the maximum number of historical searches is multiplied to determine the maximum number of concurrent real-time searches. Note: The maximum number of real-time searches is computed as max_rt_searches = max_rt_search_multiplier x max_hist_searches

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/concurrency-settings/search -d
base_max_searches=5 -d max_searches_per_cpu=4
```

XML Response

```
feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>search-concurrency-settings-handler</title>
  <id>https://localhost:8089/services/search/concurrency-settings</id>
  <updated>2019-04-21T17:31:19-07:00</updated>
  <generator build="efdccca30d13" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search</title>
    <id>https://localhost:8089/services/search/concurrency-settings/search</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/search/concurrency-settings/search" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/concurrency-settings/search" rel="list"/>
    <link href="/services/search/concurrency-settings/search" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="base_max_searches">5</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="max_rt_search_multiplier">1</s:key>
        <s:key name="max_searches_per_cpu">4</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/jobs

`https://<host>:<mPort>/services/search/jobs`

List search jobs.

For more information about this and other search endpoints, see Creating searches using the REST API in the *REST API Tutorial*.

GET

Get details of all current searches.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
cursorTime	The earliest time from which no events are later scanned. Can be used to indicate progress. See description for `doneProgress`.
custom	Custom job property. (See the search/jobs POST request for an example of how to create a custom property.) *Note:* Filtering for custom search jobs fails in a search head cluster environment. Remove the ?search=custom filter to see all search jobs including custom jobs.
delegate	For saved searches, specifies jobs that were started by the user. Defaults to scheduler.
diskUsage	The total amount of disk space used, in bytes.
dispatchState	The state of the search. Can be any of QUEUED, PARSING, RUNNING, FINALIZING, PAUSE, INTERNAL_CANCEL, USER_CANCEL, BAD_INPUT_CANCEL, QUIT, FINALIZING, FAILED, DONE.
doneProgress	A number between 0 and 1.0 that indicates the approximate progress of the search. doneProgress = (latestTime – cursorTime) / (latestTime – earliestTime)
dropCount	For real-time searches only, the number of possible events that were dropped due to the rt_queue_size (default to 100000).
earliestTime	A time string that sets the earliest (inclusive), respectively, time bounds for the search. Can be used to indicate progress. See description for `doneProgress`.
eventAvailableCount	The number of events that are available for export.
eventCount	The number of events returned by the search.
eventFieldCount	The number of fields found in the search results.
eventIsStreaming	Indicates if the events of this search are being streamed.
eventIsTruncated	Indicates if events of the search are not stored, making them unavailable from the events endpoint for the search.
eventPreviewableCount	Number of in-memory events that are not yet committed to disk. Returned if `timeline_events_preview` is enabled in `limits.conf`.
eventSearch	Subset of the entire search that is before any transforming commands. The timeline and events endpoint represents the result of this part of the search.
eventSorting	Indicates if the events of this search are sorted, and in which order.

Name	Description

	asc = ascending;
	desc = descending;
	none = not sorted

isDone	Indicates if the search has completed.
isEventPreviewEnabled	Indicates if the `timeline_events_preview` setting is enabled in `limits.conf`.
isFailed	Indicates if there was a fatal error executing the search. For example, invalid search string syntax.
isFinalized	Indicates if the search was finalized (stopped before completion).
isPaused	Indicates if the search is paused.
isPreviewEnabled	Indicates if previews are enabled.
isRealTimeSearch	Indicates if the search is a real time search.
isRemoteTimeline	Indicates if the remote timeline feature is enabled.
isSaved	Indicates that the search job is saved, storing search artifacts on disk for 7 days from the last time that the job was viewed or touched. Add or edit the `default_save_ttl` value in `limits.conf` to override the default value of 7 days.
isSavedSearch	Indicates if this is a saved search run using the scheduler.
isZombie	Indicates if the process running the search is dead, but with the search not finished.
keywords	All positive keywords used by this search. A positive keyword is a keyword that is not in a NOT clause.
label	Custom name created for this search.
latestTime	A time string that sets the latest (exclusive), respectively, time bounds for the search. Can be used to indicate progress. See description for `doneProgress`.
messages	Errors and debug messages.
numPreviews	Number of previews generated so far for this search job.
performance	A representation of the execution costs.
priority	An integer between 0-10 that indicates the search priority. The priority is mapped to the OS process priority. The higher the number the higher the priority. The priority can be changed using action parameter for POST search/jobs/{search_id}/control. For example, for the action parameter, specify `priority=5`. *Note:* In *nix systems, non-privileged users can only reduce the priority of a process.
remoteSearch	The search string that is sent to every search peer.
reportSearch	If reporting commands are used, the reporting search.
request	GET arguments that the search sends to splunkd.
resultCount	The total number of results returned by the search. In other words, this is the subset of scanned events (represented by the scanCount) that actually matches the search terms.
resultIsStreaming	Indicates if the final results of the search are available using streaming (for example, no transforming operations).
resultPreviewCount	The number of result rows in the latest preview results.

Name	Description
runDuration	Time in seconds that the search took to complete.
scanCount	The number of events that are scanned or read off disk.
searchEarliestTime	Specifies the earliest time for a search, as specified in the search command rather than the earliestTime parameter. It does not snap to the indexed data time bounds for all-time searches (something that earliestTime/latestTime does).
searchLatestTime	Specifies the latest time for a search, as specified in the search command rather than the latestTime parameter. It does not snap to the indexed data time bounds for all-time searches (something that earliestTime/latestTime does).
searchProviders	A list of all the search peers that were contacted.
sid	The search ID number.
statusBuckets	Maximum number of timeline buckets.
ttl	The time to live, or time before the search job expires after it completes.

Application usage

The user ID is implied by the authentication to the call.

Information returned for each entry includes the search job properties, such as eventCount (number of events returned), runDuration (time the search took to complete), and others. The parameters to POST /search/jobs provides details on search job properties when creating a search. Search job properties are also described in Search job properties in the Knowledge Manager Manual.

You can specify optional arguments based on the search job properties to filter the entries returned. For example, specify search=eventCount>100 as an argument to the GET operation to return searches with event counts greater than 100.

The dispatchState property is of particular interest to determine the state of a search, and can contain the following values:

```
QUEUED
 PARSING
 RUNNING
 FINALIZING
 DONE
 PAUSE
 INTERNAL_CANCEL
 USER_CANCEL
 BAD_INPUT_CANCEL
 QUIT
 FAILED
```

This operation also returns performance information for the search.

For more information refer to "View search job properties with the Search Job Inspector" in the Knowledge Manager Manual.

For more information on searches, see the Search Reference.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs --get -d search="eventCount>100"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>jobs</title>
  <id>https://localhost:8089/services/search/jobs</id>
  <updated>2011-06-21T10:12:22-07:00</updated>
  <generator version="100492"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>8</opensearch:totalResults>
  <opensearch:itemsPerPage>0</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <entry>
    <title>search  index=_internal (source=*/metrics.log* OR source=*\\metrics.log*)
group=per_sourcetype_thruput
        | chart sum(kb) by series | sort -sum(kb) | head 5</title>
    <id>https://localhost:8089/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at
_1308676200_22702c154383bbe4</id>
    <updated>2011-06-21T10:10:31.000-07:00</updated>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4"
rel="alternate"/>
    <published>2011-06-21T10:10:23.000-07:00</published>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/search.log" rel="log"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/events" rel="events"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/results" rel="results"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/results_preview" rel="results_preview"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/timeline" rel="timeline"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/summary" rel="summary"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
/control" rel="control"/>
    <author>
      <name>splunk-system-user</name>
    </author>
    <content type="text/xml">
      <s:dict>
        <s:key name="cursorTime">1969-12-31T16:00:00.000-08:00</s:key>
        <s:key name="delegate">scheduler</s:key>
        <s:key name="diskUsage">73728</s:key>
        <s:key name="dispatchState">DONE</s:key>
        <s:key name="doneProgress">1.00000</s:key>
        <s:key name="dropCount">0</s:key>
        <s:key name="earliestTime">2011-06-20T10:10:00.000-07:00</s:key>
        <s:key name="eventAvailableCount">0</s:key>
        <s:key name="eventCount">1363</s:key>
        <s:key name="eventFieldCount">0</s:key>
        <s:key name="eventIsStreaming">1</s:key>
        <s:key name="eventIsTruncated">1</s:key>
        <s:key name="eventSearch">search index=_internal (source=*/metrics.log* OR source=*\\metrics.log*)
group=per_sourcetype_thruput </s:key>
        <s:key name="eventSorting">none</s:key>
        <s:key name="isDone">1</s:key>
        <s:key name="isFailed">0</s:key>
        <s:key name="isFinalized">0</s:key>
        <s:key name="isPaused">0</s:key>
        <s:key name="isPreviewEnabled">0</s:key>
        <s:key name="isRealTimeSearch">0</s:key>
        <s:key name="isRemoteTimeline">0</s:key>
        <s:key name="isSaved">0</s:key>
        <s:key name="isSavedSearch">1</s:key>
        <s:key name="isZombie">0</s:key>
        <s:key name="keywords">group::per_sourcetype_thruput index::_internal source::*/metrics.log*
source::*\metrics.log*</s:key>
        <s:key name="label">Top five sourcetypes</s:key>
        <s:key name="latestTime">2011-06-21T10:10:00.000-07:00</s:key>
        <s:key name="numPreviews">0</s:key>
        <s:key name="priority">5</s:key>
        <s:key name="remoteSearch">litsearch index=_internal ( source=*/metrics.log* OR
source=*\\metrics.log* )
                group=per_sourcetype_thruput | addinfo  type=count label=prereport_events
                | fields  keepcolorder=t "kb" "prestats_reserved_*" "psrsvd_*" "series"
                | convert  num("kb")  | prestats  sum(kb) AS "sum(kb)" by series</s:key>
        <s:key name="reportSearch">chart  sum(kb) by series  | sort  -sum(kb)  | head  5</s:key>
        <s:key name="resultCount">4</s:key>
        <s:key name="resultIsStreaming">0</s:key>
        <s:key name="resultPreviewCount">4</s:key>
        <s:key name="runDuration">0.259000</s:key>
        <s:key name="scanCount">1363</s:key>
        <s:key name="searchEarliestTime">1308589800.000000000</s:key>
        <s:key name="searchLatestTime">1308676200.000000000</s:key>
        <s:key
name="sid">scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4</s:key>
        <s:key name="statusBuckets">0</s:key>
        <s:key name="ttl">489</s:key>
        <s:key name="performance">
          <s:dict>
            <s:key name="command.addinfo">
              <s:dict>
                <s:key name="duration_secs">0.005</s:key>
                <s:key name="invocations">5</s:key>
                <s:key name="input_count">1363</s:key>
                <s:key name="output_count">1363</s:key>
              </s:dict>
            </s:key>
            <s:key name="command.chart">
              <s:dict>
                <s:key name="duration_secs">0.003</s:key>
                <s:key name="invocations">1</s:key>
                <s:key name="input_count">100000</s:key>
                <s:key name="output_count">4</s:key>
              </s:dict>
            </s:key>
            <s:key name="command.convert">
              <s:dict>
                <s:key name="duration_secs">0.006</s:key>
```

```
    <s:key name="invocations">5</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.fields">
  <s:dict>
    <s:key name="duration_secs">0.005</s:key>
    <s:key name="invocations">5</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.head">
  <s:dict>
    <s:key name="duration_secs">0.001</s:key>
    <s:key name="invocations">1</s:key>
    <s:key name="input_count">4</s:key>
    <s:key name="output_count">4</s:key>
  </s:dict>
</s:key>
<s:key name="command.presort">
  <s:dict>
    <s:key name="duration_secs">0.001</s:key>
    <s:key name="invocations">1</s:key>
    <s:key name="input_count">4</s:key>
    <s:key name="output_count">4</s:key>
  </s:dict>
</s:key>
<s:key name="command.prestats">
  <s:dict>
    <s:key name="duration_secs">0.014</s:key>
    <s:key name="invocations">5</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">12</s:key>
  </s:dict>
</s:key>
<s:key name="command.search">
  <s:dict>
    <s:key name="duration_secs">0.058</s:key>
    <s:key name="invocations">5</s:key>
    <s:key name="input_count">0</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.fieldalias">
  <s:dict>
    <s:key name="duration_secs">0.003</s:key>
    <s:key name="invocations">3</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.filter">
  <s:dict>
    <s:key name="duration_secs">0.004</s:key>
    <s:key name="invocations">3</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.index">
  <s:dict>
    <s:key name="duration_secs">0.010</s:key>
    <s:key name="invocations">5</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.kv">
  <s:dict>
    <s:key name="duration_secs">0.011</s:key>
    <s:key name="invocations">3</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.lookups">
  <s:dict>
    <s:key name="duration_secs">0.003</s:key>
    <s:key name="invocations">3</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.rawdata">
  <s:dict>
    <s:key name="duration_secs">0.034</s:key>
    <s:key name="invocations">3</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.tags">
  <s:dict>
    <s:key name="duration_secs">0.005</s:key>
    <s:key name="invocations">5</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.search.typer">
  <s:dict>
    <s:key name="duration_secs">0.005</s:key>
    <s:key name="invocations">5</s:key>
    <s:key name="input_count">1363</s:key>
    <s:key name="output_count">1363</s:key>
  </s:dict>
</s:key>
<s:key name="command.sort">
  <s:dict>
    <s:key name="duration_secs">0.001</s:key>
    <s:key name="invocations">1</s:key>
    <s:key name="input_count">4</s:key>
    <s:key name="output_count">4</s:key>
  </s:dict>
</s:key>
<s:key name="dispatch.createProviderQueue">
  <s:dict>
    <s:key name="duration_secs">0.067</s:key>
    <s:key name="invocations">1</s:key>
  </s:dict>
</s:key>
<s:key name="dispatch.evaluate">
  <s:dict>
    <s:key name="duration_secs">0.038</s:key>
    <s:key name="invocations">1</s:key>
  </s:dict>
</s:key>
<s:key name="dispatch.evaluate.chart">
  <s:dict>
    <s:key name="duration_secs">0.001</s:key>
```

```
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.evaluate.head">
      <s:dict>
        <s:key name="duration_secs">0.001</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.evaluate.search">
      <s:dict>
        <s:key name="duration_secs">0.037</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.evaluate.sort">
      <s:dict>
        <s:key name="duration_secs">0.001</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.fetch">
      <s:dict>
        <s:key name="duration_secs">0.126</s:key>
        <s:key name="invocations">6</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.stream.local">
      <s:dict>
        <s:key name="duration_secs">0.070</s:key>
        <s:key name="invocations">5</s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:key>
<s:key name="messages">
  <s:dict/>
</s:key>
<s:key name="request">
  <s:dict>
    <s:key name="ui_dispatch_app"></s:key>
    <s:key name="ui_dispatch_view"></s:key>
  </s:dict>
</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>admin</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>admin</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="owner">nobody</s:key>
    <s:key name="modifiable">true</s:key>
```

```
            <s:key name="sharing">global</s:key>
            <s:key name="app">search</s:key>
            <s:key name="can_write">true</s:key>
          </s:dict>
        </s:key>
        <s:key name="searchProviders">
          <s:list>
            <s:item>mbp15.splunk.com</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
  . . . elided . . .
</feed>
```

POST

Start a new search and return the search ID (<sid>)

Request parameters

Name	Type	Default	Description
adhoc_search_level	String		Use one of the following search modes. `[ verbose | fast | smart ]` If `adhoc_search_level` is not specified, the default mode is `fast`.
allow_partial_results	Boolean	true	Indicates whether the search job can proceed to provide partial results if a search peer fails. When `false`, the search job fails if a search peer providing results for the search job fails.
auto_cancel	Number	0	If specified, the job automatically cancels after this many seconds of inactivity. (0 means never aut
auto_finalize_ec	Number	0	Auto-finalize the search after at least this many events are processed. Specify `0` to indicate no limit.
auto_pause	Number	0	If specified, the search job pauses after this many seconds of inactivity. (0 means never auto-paus To restart a paused search job, specify unpause as an action to POST search/jobs/{search_id}/control. auto_pause only goes into effect once. Unpausing after auto_pause does not put auto_pause into effect again.
custom	String		Specify a custom parameter (see example).
earliest_time	String		Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search. The time string can be either a UTC time (with fractional seconds), a relative time (to now) or a formatted time string. Refer to Time modifiers for search for informat examples of specifying a time string. Compare to `index_earliest` parameter. Also see comment for the `search_mode` pa
enable_lookups	Boolean	true	Indicates whether lookups should be applied to events. Specifying true (the default) may slow searches significantly depending on the nat lookups.

Name	Type	Default	Description
exec_mode	Enum	normal	Valid values: (blocking | oneshot | normal) If set to normal, runs an asynchronous search. If set to blocking, returns the sid when the job is complete. If set to oneshot, returns results in the same call. In this case, you can specify the the output (for example, json output) using the output_mode parameter as describ search/jobs/export. Default format for output is xml. Does not return the search ID
force_bundle_replication	Boolean	false	Specifies whether this search should cause (and wait depending on the value of sync_bundle_repl bundle synchronization with all search peers.
id	String		Optional string to specify the search ID (`<sid>`). If unspecified, a random ID is generated.
index_earliest	String		Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based time bounds. The time string can be either a UTC time (with fractional seconds), a relative time (to now) or a formatted time string. Compare to `earliest_time` parameter. Also se comment for the `search_mode` parameter. Refer to Time modifiers for search for information and examples of specifying a ti
index_latest	String		Specify a time string. Sets the latest (exclusive), respectively, time bounds for the search, based o time bounds. The time string can be either a UTC time (with fractional seconds), a relative time (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a ti Compare to `latest_time` parameter. Also see comment for the `search_mode` para
indexedRealtime	Boolean		Indicate whether or not to used indexed-realtime mode for real-time searches.
indexedRealtimeOffset	Number		Set disk sync delay for indexed real-time search (seconds).
latest_time	String		Specify a time string. Sets the latest (exclusive), respectively, time bounds for the search. The time string can be either a UTC time (with fractional seconds), a relative time (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a ti Compare to `index_latest` parameter. Also see comment for the `search_mode` para
max_count	Number	10000	The number of events that can be accessible in any given status bucket. Also, in transforming mode, the maximum number of results to store. Specifically, `codeoffset+count max_count.`
max_time	Number	0	The number of seconds to run this search before finalizing. Specify `0` to never finalize.
namespace	String		The application namespace in which to restrict searches.

Name	Type	Default	Description
			The namespace corresponds to the identifier recognized in the `/services/apps/l` endpoint.
now	String	current system time	Specify a time string to set the absolute time used for any relative time specifier in the search. Def current system time. You can specify a relative time modifier for this parameter. For example, specify + specify the current time plus two days. If you specify a relative time modifier both in this parameter and in the search stri search string modifier takes precedence. Refer to Time modifiers for search for details on specifying relative time modifiers.
reduce_freq	Number	0	Determines how frequently to run the MapReduce reduce phase on accumulated map values.
reload_macros	Boolean	true	Specifies whether to reload macro definitions from `macros.conf`. Default is true.
remote_server_list	String	empty list	Comma-separated list of (possibly wildcarded) servers from which raw events should be pulled. Th server list is to be used in subsearches.

replay_speed	Number greater than 0		Indicate a real-time search replay speed factor. For example, `1` indicates normal speed. `0.5` indica normal speed, and `2` indicates twice as fast as normal.
			`earliest_time` and `latest_time` arguments must indicate a real-time time range t replay options.
			Use *replay_speed* with *replay_et* and *replay_lt* relative times to indicate a speed a range for the replay. For example,
			`replay_speed = 10`
			`replay_et = -d@d`
			`replay_lt = -@d`
			specifies a replay at 10x speed, as if the "wall clock" time starts yesterday at midn ends when it reaches today at midnight.
			For more information about using relative time modifiers, see Search time modifie *Search reference*.

replay_et	Time modifier string		Relative "wall clock" start time for the replay.
replay_lt	Time modifier string.		Relative end time for the replay clock. The replay stops when clock time reaches this time.
required_field_list	String	empty list	[Deprecated] Use *rf*. A comma-separated list of required fields that, even if not referenced or used dire search, is still included by the events and summary endpoints. Splunk Web uses t to prepopulate panels in the Search view.

Name	Type	Default	Description
reuse_max_seconds_ago	Number		Specifies the number of seconds ago to check when an identical search is started and return the jo ID instead of starting a new job.
rf	String		Adds a required field to the search. There can be multiple `rf` POST arguments to the search. These fields, even if not referenced or used directly by the search, are still include events and summary endpoints. Splunk Web uses these fields to prepopulate par Search view. Consider using this form of passing the required fields to the search instead of the deprecated *required_field_list*. If both *rf* and *required_field_list* are provided, the u two lists is used.
rt_blocking	Boolean	false	For a real-time search, indicates if the indexer blocks if the queue for this search is full.
rt_indexfilter	Boolean	true	For a real-time search, indicates if the indexer prefilters events.
rt_maxblocksecs	Number	60	For a real-time search with rt_blocking set to true, the maximum time to block. Specify `0` to indicate no limit.
rt_queue_size	Number	10000 events	For a real-time search, the queue size (in events) that the indexer should use for this search.

search
required
	String		The search language string to execute, taking results from the local and remote servers.
			Examples:
			`"search *"`
			`"search * | outputcsv"`

search_listener	String		[Disabled] Registers a search state listener with the search. Use the format: search_state;results_condition;http_method;uri; For example: search_listener=onResults;true;POST;/servicesNS/admin/search/saved/search/fo
search_mode	Enum	normal	Valid values: (normal | realtime) If set to `realtime`, search runs over live data. A real-time search may also be indic earliest_time and latest_time variables starting with 'rt' even if the search_mode is normal or is unset. For a real-time search, if both earliest_time and latest_time are exactly 'rt', the search represents all appropriate live data received since the start search. Additionally, if earliest_time and/or latest_time are 'rt' followed by a relative time s then a sliding window is used where the time bounds of the window are determine relative time specifiers and are continuously updated based on the wall-clock time

Name	Type	Default	Description
spawn_process	Boolean	true	This parameter is deprecated and will be removed in a future release. Do not use this parameter. Specifies whether the search should run in a separate spawned process. Default Searches against indexes *must* run in a separate process.
status_buckets	Number	0	The most status buckets to generate. `0` indicates to not generate timeline information.
sync_bundle_replication	Boolean		Specifies whether this search should wait for bundle replication to complete.
time_format	String	%FT%T.%Q%:z	Used to convert a formatted time string from {start,end}_time into UTC seconds. The default value ISO-8601 format.
timeout	Number	86400	The number of seconds to keep this search after processing has stopped.
workload_pool	String		Specifies the new workload pool where the existing running search should be placed.

Returned values

Name	Description
sid	Search ID

Application usage

Refer to Creating searches using the REST API for information on using this endpoint and other search endpoints.

The search parameter is a search language string that specifies the search. Often you create a search specifying just the search parameter. Use the other parameters to customize a search to specific needs.

Use the returned (<sid>) in the following endpoints to view and manage the search:

```
  search/jobs/{search_id}: View the status of this search job.
   search/jobs/{search_id}/control: Execute job control commands, such as pause, cancel, preview, and
others.
   search/jobs/{search_id}/events: View a set of untransformed events for the search.
   search/jobs/{search_id}/results: View results of the search.
   search/jobs/{search_id}/results_preview: Preview results of a search that has not completed
   search/jobs/{search_id}/search.log: View the log file generated by the search.
   search/jobs/{search_id}/summary: View field summary information
   search/jobs/{search_id}/timeline: View event distribution over time.
```

You can also use the custom attribute to create custom job properties (see example).

For more information on searches, see the Splunk Search Reference.

Example request and response

Request

- Basic example:

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/jobs --data-urlencode
search="search index=_internal source=*/metrics.log" -d id=mysearch_02151949 -d max_count=50000 -d
status_buckets=300
```

- Create custom property example:

```
curl -u admin:changeme -k https://localhost:8089/services/search/jobs
    -d search="search *"
    -d custom.foobar="myCustomPropA"
    -d custom.foobaz="myCustomPropB"
```

Use the search/jobs GET request to view the custom properties.

- Create indexed real-time search with five second disk sync delay example:

```
curl -k -u admin:changed https://localhost:8089/services/search/jobs
    -d search="search index=_* *"
    -d search_mode="realtime"
    -d indexedRealtime="1"
    -d indexedRealtimeOffset="300"
```

Response

```
<response><sid>mysearch_02151949</sid></response>
```

search/v2/jobs/export

```
https://<host>:<mPort>/services/search/v2/jobs/export
```

Stream search results as they become available.

The POST operation on this endpoint performs a search identical to a POST to `search/jobs`. For parameter and returned value descriptions, see search/jobs.

The GET operation is not available in the v2 iteration of this endpoint.

POST

Performs a search identical to POST search/jobs. For parameter and returned value descriptions, see the POST parameter descriptions for search/jobs.

Request parameters

Name	Type	Default	Description
search	String		See the parameters and returned values for search/jobs.
auto_cancel	Number		See the parameters and returned values for search/jobs.
auto_finalize_ec	Number		See the parameters and returned values for search/jobs.
auto_pause	Number		See the parameters and returned values for search/jobs.
earliest_time	String		See the parameters and returned values for search/jobs.

Name	Type	Default	Description
enable_lookups	Bool		See the parameters and returned values for search/jobs.
force_bundle_replication	Bool		See the parameters and returned values for search/jobs.
id	String		See the parameters and returned values for search/jobs.
index_earliest	String		Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
index_latest	String		Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
latest_time	String		See the parameters and returned values for search/jobs.
max_time	Number		See the parameters and returned values for search/jobs.
namespace	String		See the parameters and returned values for search/jobs.
now	String		See the parameters and returned values for search/jobs.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
reduce_freq	Number		See the parameters and returned values for search/jobs.
reload_macros	Bool		See the parameters and returned values for search/jobs.
remote_server_list	String		See the parameters and returned values for search/jobs.
required_field_list	String		See the parameters and returned values for search/jobs.
rf	String		See the parameters and returned values for search/jobs.
rt_blocking	Bool		See the parameters and returned values for search/jobs.
rt_indexfilter	Bool		See the parameters and returned values for search/jobs.
rt_maxblocksecs	Number		See the parameters and returned values for search/jobs.
rt_queue_size	Number		See the parameters and returned values for search/jobs.
search_listener	String		See the parameters and returned values for search/jobs.
search_mode	Enum		See the parameters and returned values for search/jobs.
sync_bundle_replication	Bool		See the parameters and returned values for search/jobs.
time_format	String		See the parameters and returned values for search/jobs.

Name	Type	Default	Description
timeout	Number		See the parameters and returned values for search/jobs.

Returned values
None

Application usage
Streaming of results is based on the search string.

For non-streaming searches, previews of the final results are available if preview is enabled. If preview is not enabled, use search/jobs with exec_mode=oneshot.

If your search is too big, considering running it with the search/jobs endpoint, instead of the search/jobs/export endpoint, and using exec_mode=blocking. You'll then get back a search id, and then you can page through the results and request them from the server under your control. This is a better approach for extremely large result sets that need to be chunked.

Example

The following example runs a saved search and passes a variable to it. In this case, the variable is the host field:

```
$curl -k -u admin:password https://splunkserver:8089/services/search/v2/jobs/export -d search="savedsearch
\ MySavedSearch%20host%3Dwolverine*"
```

This request creates a saved search named "MySavedSearch" which contains the following result:

```
"index=main $host$ | head 100"
```

search/jobs/export (deprecated)

```
https://<host>:<mPort>/services/search/jobs/export
```

Stream search results as they become available.

The GET and POST operations on this endpoint perform a search identical to a POST to `search/jobs`. For parameter and returned value descriptions, see search/jobs.

This endpoint is deprecated as of Splunk Enterprise 9.0.1. Use the v2 instance of this endpoint instead.

GET

Performs a search identical to POST search/jobs

Request parameters
See the POST operation on search/jobs for parameter descriptions.

Name	Type	Default	Description

Name	Type	Default	Description
auto_cancel	Number		See the POST parameter descriptions for search/jobs
auto_finalize_ec	Number		See the POST parameter descriptions for search/jobs
auto_pause	Number		See the POST parameter descriptions for search/jobs
earliest_time	String		See the POST parameter descriptions for search/jobs
enable_lookups	Bool		See the POST parameter descriptions for search/jobs
force_bundle_replication	Bool		See the POST parameter descriptions for search/jobs
id	String		See the POST parameter descriptions for search/jobs
index_earliest	String		Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
index_latest	String		Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
latest_time	String		See the POST parameter descriptions for search/jobs
max_time	Number		See the POST parameter descriptions for search/jobs
namespace	String		See the POST parameter descriptions for search/jobs
now	String		See the POST parameter descriptions for search/jobs
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
reduce_freq	Number		See the POST parameter descriptions for search/jobs
reload_macros	Bool		See the POST parameter descriptions for search/jobs
remote_server_list	String		See the POST parameter descriptions for search/jobs
required_field_list	String		See the POST parameter descriptions for search/jobs
rf	String		See the POST parameter descriptions for search/jobs
rt_blocking	Bool		See the POST parameter descriptions for search/jobs
rt_indexfilter	Bool		See the POST parameter descriptions for search/jobs
rt_maxblocksecs	Number		See the POST parameter descriptions for search/jobs
rt_queue_size	Number		See the POST parameter descriptions for search/jobs

Name	Type	Default	Description
search required	String		See the POST parameter descriptions for search/jobs
search_listener	String		See the POST parameter descriptions for search/jobs
search_mode	Enum		See the POST parameter descriptions for search/jobs
sync_bundle_replication	Bool		See the POST parameter descriptions for search/jobs
time_format	String		See the POST parameter descriptions for search/jobs
timeout	Number		See the POST parameter descriptions for search/jobs

Returned values

None

Application usage

Performs a search identical to POST `search/jobs`, except the search streams results as they become available. Streaming of results is based on the search string.

For non-streaming searches, previews of the final results are available if preview is enabled. If preview is not enabled, use the `search/jobs` endpoint with `exec_mode=oneshot` to retrieve results from them.

If the result set returned by a non-streaming search is significantly large, use the `search/jobs` endpoint with `exec_mode=blocking`. This approach lets you page through the results and request them from a server under your control.

Example request and response

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/jobs/export -d search="search
index%3D_internal | head 1"
```

XML Response

```
<results preview='0'>
<meta>
<fieldOrder>
<field>_cd</field>
<field>_indextime</field>
<field>_raw</field>
<field>_serial</field>
<field>_si</field>
<field>_sourcetype</field>
<field>_subsecond</field>
<field>_time</field>
<field>host</field>
<field>index</field>
<field>linecount</field>
<field>source</field>
<field>sourcetype</field>
<field>splunk_server</field>
</fieldOrder>
</meta>
<messages>
  <msg type="DEBUG">base lispy: [ AND index::_internal ]</msg>
  <msg type="DEBUG">search context: user="admin", app="search",
bs-pathname="/Applications/splunk/etc"</msg>
  <msg type="INFO">Your timerange was substituted based on your search string</msg>
```

```
</messages>

  <result offset='0'>
    <field k='_cd'>
      <value><text>50:59480</text></value>
    </field>
    <field k='_indextime'>
      <value><text>1333739623</text></value>
    </field>
    <field k='_raw'><v xml:space='preserve' trunc='0'>127.0.0.1 - admin [06/Apr/2012:12:13:42.943 -0700]
"POST /servicesNS/admin/search/search/jobs/export HTTP/1.1" 200 2063 - - - 317ms</v></field>
    <field k='_serial'>
      <value><text>0</text></value>
    </field>
    <field k='_si'>
      <value><text>mbp15.splunk.com</text></value>
      <value><text>_internal</text></value>
    </field>
    <field k='_sourcetype'>
      <value><text>splunkd_access</text></value>
    </field>
    <field k='_subsecond'>
      <value><text>.943</text></value>
    </field>
    <field k='_time'>
      <value><text>2012-04-06 12:13:42.943 PDT</text></value>
    </field>
    <field k='host'>
      <value><text>mbp15.splunk.com</text></value>
    </field>
    <field k='index'>
      <value h='1'><text>_internal</text></value>
    </field>
    <field k='linecount'>
      <value><text>1</text></value>
    </field>
    <field k='source'>
      <value><text>/Applications/splunk/var/log/splunk/splunkd_access.log</text></value>
    </field>
    <field k='sourcetype'>
      <value><text>splunkd_access</text></value>
    </field>
    <field k='splunk_server'>
      <value><text>mbp15.splunk.com</text></value>
    </field>
  </result>
</results>
```

POST

Performs a search identical to POST search/jobs. For parameter and returned value descriptions, see the POST parameter descriptions for search/jobs.

Request parameters

Name	Type	Default	Description
search	String		See the parameters and returned values for search/jobs.
auto_cancel	Number		See the parameters and returned values for search/jobs.
auto_finalize_ec	Number		See the parameters and returned values for search/jobs.

Name	Type	Default	Description
auto_pause	Number		See the parameters and returned values for search/jobs.
earliest_time	String		See the parameters and returned values for search/jobs.
enable_lookups	Bool		See the parameters and returned values for search/jobs.
force_bundle_replication	Bool		See the parameters and returned values for search/jobs.
id	String		See the parameters and returned values for search/jobs.
index_earliest	String		Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
index_latest	String		Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
latest_time	String		See the parameters and returned values for search/jobs.
max_time	Number		See the parameters and returned values for search/jobs.
namespace	String		See the parameters and returned values for search/jobs.
now	String		See the parameters and returned values for search/jobs.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
reduce_freq	Number		See the parameters and returned values for search/jobs.
reload_macros	Bool		See the parameters and returned values for search/jobs.
remote_server_list	String		See the parameters and returned values for search/jobs.
required_field_list	String		See the parameters and returned values for search/jobs.
rf	String		See the parameters and returned values for search/jobs.
rt_blocking	Bool		See the parameters and returned values for search/jobs.
rt_indexfilter	Bool		See the parameters and returned values for search/jobs.
rt_maxblocksecs	Number		See the parameters and returned values for search/jobs.
rt_queue_size	Number		See the parameters and returned values for search/jobs.
search_listener	String		See the parameters and returned values for search/jobs.
search_mode	Enum		See the parameters and returned values for search/jobs.

Name	Type	Default	Description
sync_bundle_replication	Bool		See the parameters and returned values for search/jobs.
time_format	String		See the parameters and returned values for search/jobs.
timeout	Number		See the parameters and returned values for search/jobs.

Returned values
None

Application usage
Streaming of results is based on the search string.

For non-streaming searches, previews of the final results are available if preview is enabled. If preview is not enabled, it is better to use search/jobs with exec_mode=oneshot.

If it is too big, you might instead run with the search/jobs (not search/jobs/export) endpoint (it takes POST with the same parameters), maybe using the exec_mode=blocking. You'll then get back a search id, and then you can page through the results and request them from the server under your control, which is a better approach for extremely large result sets that need to be chunked.

Example of how to pass a variable to query when using REST API:

This is an example of running a saved search and passing a variable to it. In this case, the variable is host field:

```
$curl -k -u admin:password https://splunkserver:8089/services/search/jobs/export -d search="savedsearch \
MySavedSearch%20host%3Dwolverine*"
```

(use "MySavedSearch" and input variable host=wolverine*)

I have a saved search named "MySavedSearch" the query of the search contains:

"index=main $host$ | head 100"

search/jobs/{search_id}

```
https://<host>:<mPort>/services/search/jobs/{search_id}
```

Manage the `{search_id}` search job.

DELETE

Delete the `{search_id}` search job.

Request parameters
None

Returned values
None

Application usage
{search_id} is the <sid> field returned from the GET operation for the search/jobs endpoint.

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/services/search/jobs/mysearch_02151949
```

XML Response

```
<response><messages><msg type='INFO'>Search job cancelled.</msg></messages></response
```

GET

Get information about the `{search_id}` search job.

Request parameters
None

Returned values
None

Application usage
The user ID is implied by the authentication to the call.

Information returned includes the search job properties, such as eventCount (number of events returned), runDuration (time the search took to complete), and others. The parameters to POST /search/jobs provides details on search job properties when creating a search. Search job properties are also described in View search job properties in the *Search Manual*.

The dispatchState property is of particular interest to determine the state of a search, and can contain the following values:

```
QUEUED
 PARSING
 RUNNING
 FINALIZING
 DONE
 PAUSE
 INTERNAL_CANCEL
 USER_CANCEL
 BAD_INPUT_CANCEL
 QUIT
 FAILED
```

This operation also returns performance information for the search. For more information refer to View search job properties in the *Search Manual*.

For more information on searches in Splunk, refer to the Splunk Search Reference.

POST /search/jobs returns a <sid> for a search. You can also get a search ID from the <sid> field returned from GET search/jobs.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949
```

XML Response

```
<entry
       xmlns="http://www.w3.org/2005/Atom"
       xmlns:s="http://dev.splunk.com/ns/rest"
       xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>search index</title>
  <id>https://localhost:8089/services/search/jobs/mysearch_02151949</id>
  <updated>2011-07-07T20:49:58.000-07:00</updated>
  <link href="/services/search/jobs/mysearch_02151949" rel="alternate"/>
  <published>2011-07-07T20:49:57.000-07:00</published>
  <link href="/services/search/jobs/mysearch_02151949/search.log" rel="search.log"/>
  <link href="/services/search/jobs/mysearch_02151949/events" rel="events"/>
  <link href="/services/search/jobs/mysearch_02151949/results" rel="results"/>
  <link href="/services/search/jobs/mysearch_02151949/results_preview" rel="results_preview"/>
  <link href="/services/search/jobs/mysearch_02151949/timeline" rel="timeline"/>
  <link href="/services/search/jobs/mysearch_02151949/summary" rel="summary"/>
  <link href="/services/search/jobs/mysearch_02151949/control" rel="control"/>
  <author>
    <name>admin</name>
  </author>
  <content type="text/xml">
    <s:dict>
      <s:key name="cursorTime">1969-12-31T16:00:00.000-08:00</s:key>
      <s:key name="delegate"></s:key>
      <s:key name="diskUsage">2174976</s:key>
      <s:key name="dispatchState">DONE</s:key>
      <s:key name="doneProgress">1.00000</s:key>
      <s:key name="dropCount">0</s:key>
      <s:key name="earliestTime">2011-07-07T11:18:08.000-07:00</s:key>
      <s:key name="eventAvailableCount">287</s:key>
      <s:key name="eventCount">287</s:key>
      <s:key name="eventFieldCount">6</s:key>
      <s:key name="eventIsStreaming">1</s:key>
      <s:key name="eventIsTruncated">0</s:key>
      <s:key name="eventSearch">search index</s:key>
      <s:key name="eventSorting">desc</s:key>
      <s:key name="isDone">1</s:key>
      <s:key name="isFailed">0</s:key>
      <s:key name="isFinalized">0</s:key>
      <s:key name="isPaused">0</s:key>
      <s:key name="isPreviewEnabled">0</s:key>
      <s:key name="isRealTimeSearch">0</s:key>
      <s:key name="isRemoteTimeline">0</s:key>
      <s:key name="isSaved">0</s:key>
      <s:key name="isSavedSearch">0</s:key>
      <s:key name="isZombie">0</s:key>
      <s:key name="keywords">index</s:key>
      <s:key name="label"></s:key>
      <s:key name="latestTime">1969-12-31T16:00:00.000-08:00</s:key>
      <s:key name="numPreviews">0</s:key>
      <s:key name="priority">5</s:key>
      <s:key name="remoteSearch">litsearch index | fields  keepcolorder=t "host" "index" "linecount"
"source" "sourcetype" "splunk_server"</s:key>
      <s:key name="reportSearch"></s:key>
      <s:key name="resultCount">287</s:key>
      <s:key name="resultIsStreaming">1</s:key>
      <s:key name="resultPreviewCount">287</s:key>
      <s:key name="runDuration">1.004000</s:key>
      <s:key name="scanCount">287</s:key>
      <s:key name="sid">mysearch_02151949</s:key>
      <s:key name="statusBuckets">0</s:key>
      <s:key name="ttl">516</s:key>
      <s:key name="performance">
        <s:dict>
          <s:key name="command.fields">
            <s:dict>
              <s:key name="duration_secs">0.004</s:key>
              <s:key name="invocations">4</s:key>
              <s:key name="input_count">287</s:key>
              <s:key name="output_count">287</s:key>
            </s:dict>
          </s:key>
          <s:key name="command.search">
            <s:dict>
              <s:key name="duration_secs">0.089</s:key>
              <s:key name="invocations">4</s:key>
              <s:key name="input_count">0</s:key>
              <s:key name="output_count">287</s:key>
            </s:dict>
          </s:key>
          <s:key name="command.search.fieldalias">
            <s:dict>
              <s:key name="duration_secs">0.002</s:key>
              <s:key name="invocations">2</s:key>
              <s:key name="input_count">287</s:key>
              <s:key name="output_count">287</s:key>
            </s:dict>
          </s:key>
          <s:key name="command.search.index">
            <s:dict>
              <s:key name="duration_secs">0.005</s:key>
              <s:key name="invocations">4</s:key>
            </s:dict>
          </s:key>
          <s:key name="command.search.kv">
            <s:dict>
              <s:key name="duration_secs">0.002</s:key>
              <s:key name="invocations">2</s:key>
            </s:dict>
          </s:key>
          <s:key name="command.search.lookups">
            <s:dict>
              <s:key name="duration_secs">0.002</s:key>
              <s:key name="invocations">2</s:key>
              <s:key name="input_count">287</s:key>
              <s:key name="output_count">287</s:key>
            </s:dict>
          </s:key>
          <s:key name="command.search.rawdata">
            <s:dict>
              <s:key name="duration_secs">0.083</s:key>
              <s:key name="invocations">2</s:key>
            </s:dict>
```

```
    </s:key>
    <s:key name="command.search.tags">
      <s:dict>
        <s:key name="duration_secs">0.004</s:key>
        <s:key name="invocations">4</s:key>
        <s:key name="input_count">287</s:key>
        <s:key name="output_count">287</s:key>
      </s:dict>
    </s:key>
    <s:key name="command.search.typer">
      <s:dict>
        <s:key name="duration_secs">0.004</s:key>
        <s:key name="invocations">4</s:key>
        <s:key name="input_count">287</s:key>
        <s:key name="output_count">287</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.createProviderQueue">
      <s:dict>
        <s:key name="duration_secs">0.059</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.evaluate">
      <s:dict>
        <s:key name="duration_secs">0.037</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.evaluate.search">
      <s:dict>
        <s:key name="duration_secs">0.036</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.fetch">
      <s:dict>
        <s:key name="duration_secs">0.092</s:key>
        <s:key name="invocations">5</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.readEventsInResults">
      <s:dict>
        <s:key name="duration_secs">0.110</s:key>
        <s:key name="invocations">1</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.stream.local">
      <s:dict>
        <s:key name="duration_secs">0.089</s:key>
        <s:key name="invocations">4</s:key>
      </s:dict>
    </s:key>
    <s:key name="dispatch.timeline">
      <s:dict>
        <s:key name="duration_secs">0.359</s:key>
        <s:key name="invocations">5</s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:key>
<s:key name="messages">
```

```
        <s:dict/>
      </s:key>
      <s:key name="request">
        <s:dict>
          <s:key name="id">mysearch_02151949</s:key>
          <s:key name="search">search index</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="modifiable">true</s:key>
          <s:key name="sharing">global</s:key>
          <s:key name="app">search</s:key>
          <s:key name="can_write">true</s:key>
        </s:dict>
      </s:key>
      <s:key name="searchProviders">
        <s:list>
          <s:item>mbp15.splunk.com</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
```

POST

Update the `{search_id}` search job.

Request parameters

Name	Type	Default	Description
*custom.** required	String		Specify custom job properties for the specified search job.

Returned values

None

search/jobs/{search_id}/control

`https://<host>:<mPort>/services/search/jobs/{search_id}/control`

Run a job control command for the `{search_id}` search.

POST

Run a job control command for the `{search_id}` search.

Request parameters

Name	Type	Default	Description
action required	Enum		Valid values: (pause | unpause | finalize | cancel | touch | setttl | setpriority | enablepreview | disablepreview | setworkloadpool) The control action to execute. pause: Suspends the execution of the current search. unpause: Resumes the execution of the current search, if paused. finalize: Stops the search, and provides intermediate results to the /results endpoint. cancel: Stops the current search and deletes the result cache. touch: Extends the expiration time of the search to now + ttl setttl: Change the ttl of the search. Arguments: ttl=<number> setpriority: Sets the priority of the search process. Arguments: priority=<0-10> enablepreview: Enable preview generation (may slow search considerably). disablepreview: Disable preview generation. setworkloadpool: Moves a running search to a new workload pool. Arguments: workload_pool=<string>. Specifies the new workload pool. Requires edit_workload_pools capability. save: saves the search job, storing search artifacts on disk for 7 days. Add or edit the default_save_ttl value in limits.conf to override the default value of 7 days. unsave: Disables any action performed by save.

Returned values

None

Example request and response
XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/control -d action=pause
```

XML Response

```
<response><messages><msg type='INFO'>Search job paused.</msg></messages></response>
```

search/v2/jobs/{search_id}/events

`https://<host>:<mPort>/services/search/v2/jobs/{search_id}/events`

Access `{search_id}` search events.

The GET operation does not include the *search* parameter in the v2 iteration of this endpoint. To use the *search* parameter, use the POST operation instead.

GET

Get `{search_id}` search events.

Request parameters

Name	Type	Default	Description
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned. Default value is `100`.
earliest_time	String		A time string representing the earliest (inclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided, the union of the lists is used.
field_list	String	*	[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
latest_time	String		A time string representing the latest (exclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.
max_lines	Number	0	The maximum lines that any single event _raw field should contain. Specify `0` to specify no limit.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0.

Name	Type	Default	Description
			In 4.1+, negative offsets are allowed and are added to `count` to compute the absolute offset (for example, `offset=-1` is the last available offset. Offsets in the results are always absolute and never negative.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
output_time_format	String	`time_format`	Formats a UTC time. Defaults to what is specified in `time_format`.
segmentation	String	raw	The type of segmentation to perform on the data. This includes an option to perform k/v segmentation.
time_format	String	%m/%d/%Y:%H:%M:%S	Expression to convert a formatted time string from {start,end}_time into UTC seconds.
truncation_mode	Enum	abstract	Valid values: (abstract | truncate) Specifies how "max_lines" should be achieved.

Returned values

None

Application usage

These events are the data from the search pipeline before the first "transforming" search command. This is the primary method for a client to fetch a set of UNTRANSFORMED events for the search job.

This endpoint is only valid if the status_buckets > 0 or the search has no transforming commands.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/v2/jobs/1312313809.20/events --get -d f=arch -d
f=build -d f=connectionType -d r -d count=3
```

XML Response

```
<results preview='0'>
<meta>
<fieldOrder>
<field>arch</field>
<field>build</field>
<field>connectionType</field>
<field>date_hour</field>
</fieldOrder>
</meta>
  <result offset='0'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='1'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='2'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
</results>
```

POST

Access `{search_id}` search events.

Request parameters

Name	Type	Default	Description
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned. Default value is `100`.
earliest_time	String		A time string representing the earliest (inclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided, the union of the lists is used.
field_list	String	`*`	[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
latest_time	String		

Name	Type	Default	Description
			A time string representing the latest (exclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.
max_lines	Number	0	The maximum lines that any single event _raw field should contain. Specify `0` to specify no limit.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to `count` to compute the absolute offset (for example, `offset=-1` is the last available offset. Offsets in the results are always absolute and never negative.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
output_time_format	String	`time_format`	Formats a UTC time. Defaults to what is specified in `time_format`.
search	String		The post processing search to apply to results. Can be any valid search language string. Only usable from POST operations.
segmentation	String	raw	The type of segmentation to perform on the data. This includes an option to perform k/v segmentation.
time_format	String	%m/%d/%Y:%H:%M:%S	Expression to convert a formatted time string from {start,end}_time into UTC seconds.
truncation_mode	Enum	abstract	Valid values: (abstract | truncate) Specifies how "max_lines" should be achieved.

Returned values

None

Application usage

These events are the data from the search pipeline before the first "transforming" search command. This is the primary method for a client to fetch a set of UNTRANSFORMED events for the search job.

This endpoint is only valid if the status_buckets > 0 or the search has no transforming commands.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/v2/jobs/1312313809.20/events --get -d f=arch -d
f=build -d f=connectionType -d r -d count=3
```

XML Response

```
<results preview='0'>
<meta>
<fieldOrder>
<field>arch</field>
```

```
<field>build</field>
<field>connectionType</field>
<field>date_hour</field>
</fieldOrder>
</meta>
  <result offset='0'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='1'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='2'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
</results>
```

search/jobs/{search_id}/events (deprecated)

`https://<host>:<mPort>/services/search/jobs/{search_id}/events`

Get `{search_id}` search events.

This endpoint is deprecated as of Splunk Enterprise 9.0.1. Use the v2 instance of this endpoint instead.

GET

Access {search_id} search events.

Request parameters

Name	Type	Default	Description
count	Number	100	The maximum number of results to return. If value is set to 0, then all available results are returned. Default value is 100.
earliest_time	String		A time string representing the earliest (inclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.
f	String		A field to return for the event set. You can pass multiple POST f arguments if multiple field are required. If field_list and f are provided, the union of the lists is used.
field_list	String	*	[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
latest_time	String		A time string representing the latest (exclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.
max_lines	Number	0	The maximum lines that any single event _raw field should contain. Specify 0 to specify no limit.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to count to compute the absolute offset (for example, offset=-1 is the last available offset. Offsets in the results are always absolute and never negative.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
output_time_format	String	time_format	Formats a UTC time. Defaults to what is specified in time_format.
search	String		The post processing search to apply to results. Can be any valid search language string.
segmentation	String	raw	The type of segmentation to perform on the data. This includes an option to perform k/v segmentation.
time_format	String	%m/%d/%Y:%H:%M:%S	Expression to convert a formatted time string from {start,end}_time into UTC seconds.
truncation_mode	Enum	abstract	Valid values: (abstract | truncate) Specifies how "max_lines" should be achieved.

Returned values

None

Application usage

These events are the data from the search pipeline before the first "transforming" search command. This is the primary method for a client to fetch a set of UNTRANSFORMED events for the search job.

This endpoint is only valid if the status_buckets > 0 or the search has no transforming commands.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/1312313809.20/events --get -d f=arch -d
f=build -d f=connectionType -d r -d count=3
```

XML Response

```
<results preview='0'>
<meta>
<fieldOrder>
<field>arch</field>
<field>build</field>
<field>connectionType</field>
<field>date_hour</field>
</fieldOrder>
</meta>
  <result offset='0'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='1'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='2'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
```

```
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
</results>
```

search/v2/jobs/{search_id}/results

`https://<host>:<mPort>/services/search/v2/jobs/{search_id}/results`

Access `{search_id}` search results.

The GET operation does not include the *search* parameter in the v2 iteration of this endpoint. To use the *search* parameter, use the POST operation instead.

GET

Get `{search_id}` search results.

Request parameters

Name	Type	Default	Description
add_summary_to_metadata	Boolean	false	Set the value to "true" to include field summary statistics in the response.
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided the union of the lists is used.
field_list	String		[Deprecated] Use *f*. Specify a comma-separated list of the fields to return for the event set.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to `count` to compute the absolute offset (for example, `offset=-1` is the last available offset). Offsets in the results are always absolute and never negative.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.

Returned values

None

Application usage

This is the table that exists after all processing from the search pipeline has completed.

This is the primary method for a client to fetch a set of TRANSFORMED events. If the dispatched search does not include a transforming command, the effect is the same as get_events, however with fewer options.

Example request and response

JSON request

```
curl -k -u admin:pass https://localhost:8089/services/search/v2/jobs/mysearch_02151949/results --get -d
f=index -d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

JSON response

```
{ "init_offset" : 0,
  "messages" : [ { "text" : "base lispy: [ AND index::_internal source::*/metrics.log ]",
        "type" : "DEBUG"
      },
      { "text" : "search context: user=\"admin\", app=\"search\",
bs-pathname=\"/Applications/splunk/etc\"",
        "type" : "DEBUG"
      }
    ],
  "preview" : false,
  "results" : [ { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      }
    ]
}
```

POST

Access `{search_id}` search results.

Request parameters

Name	Type	Default	Description
add_summary_to_metadata	Boolean	false	Set the value to "true" to include field summary statistics in the response.
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned.
f	String		A field to return for the event set.

Name	Type	Default	Description
			You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided the union of the lists is used.
field_list	String		[Deprecated] Use *f*. Specify a comma-separated list of the fields to return for the event set.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to `count` to compute the absolute offset (for example, `offset=-1` is the last available offset). Offsets in the results are always absolute and never negative.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
search	String		The post processing search to apply to results. Can be any valid search language string. Only usable from POST operations.

Returned values

None

Application usage

This is the table that exists after all processing from the search pipeline has completed.

This is the primary method for a client to fetch a set of TRANSFORMED events. If the dispatched search does not include a transforming command, the effect is the same as get_events, however with fewer options.

Example request and response

JSON request

```
curl -k -u admin:pass https://localhost:8089/services/search/v2/jobs/mysearch_02151949/results -d f=index -d
f=source -d f=sourcetype -d count=3 -d output_mode=json
```

JSON response

```
{ "init_offset" : 0,
  "messages" : [ { "text" : "base lispy: [ AND index::_internal source::*/metrics.log ]",
        "type" : "DEBUG"
      },
      { "text" : "search context: user=\"admin\", app=\"search\",
bs-pathname=\"/Applications/splunk/etc\"",
        "type" : "DEBUG"
      }
    ],
  "preview" : false,
  "results" : [ { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      }
    ]
}
```

search/jobs/{search_id}/results (deprecated)

`https://<host>:<mPort>/services/search/jobs/{search_id}/results`
Get `{search_id}` search results.

> This endpoint is deprecated as of Splunk Enterprise 9.0.1. Use the v2 instance of this endpoint instead.

GET

Get `{search_id}` search results.

Request parameters

Name	Type	Default	Description
add_summary_to_metadata	Boolean	false	Set the value to "true" to include field summary statistics in the response.
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided the union of the lists is used.
field_list	String		[Deprecated] Use *f*. Specify a comma-separated list of the fields to return for the event set.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to `count` to compute the absolute offset (for example, `offset=-1` is the last available offset). Offsets in the results are always absolute and never negative.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
search	String		The post processing search to apply to results. Can be any valid search language string.

Returned values

None

Application usage

This is the table that exists after all processing from the search pipeline has completed.

This is the primary method for a client to fetch a set of TRANSFORMED events. If the dispatched search does not include a transforming command, the effect is the same as get_events, however with fewer options.

Example request and response

JSON request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/results --get -d f=index
-d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

JSON response

```
{ "init_offset" : 0,
  "messages" : [ { "text" : "base lispy: [ AND index::_internal source::*/metrics.log ]",
        "type" : "DEBUG"
      },
      { "text" : "search context: user=\"admin\", app=\"search\",
bs-pathname=\"/Applications/splunk/etc\"",
        "type" : "DEBUG"
      }
    ],
  "preview" : false,
  "results" : [ { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      }
    ]
}
```

search/v2/jobs/{search_id}/results_preview

`https://<host>:<mPort>/services/search/v2/jobs/{search_id}/results_preview`

Preview `{search_id}` search results.

The GET operation does not include the *search* parameter in the v2 iteration of this endpoint. To use the *search* parameter, use the POST operation instead.

GET

Preview `{search_id}` search results.

Request parameters

Name	Type	Default	Description
add_summary_to_metadata	Boolean	false	Set the value to "true" to include field summary statistics in the response.
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided the union of the lists is used.
field_list	String		[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.

Returned values

None

Application usage

Returns the intermediate preview results of the search specified by {search_id}. When the job is complete, this gives the same response as /search/jobs/{search_id}/results. Preview is enabled for real-time searches and for searches where status_buckets > 0.

Example request and response

JSON request

```
curl -k -u admin:pass https://localhost:8089/services/search/v2/jobs/mysearch_02151949/results_preview --get
-d f=index -d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

JSON response

```
{ "init_offset" : 0,
  "messages" : [ { "text" : "base lispy: [ AND index::_internal source::*/metrics.log ]",
        "type" : "DEBUG"
      },
      { "text" : "search context: user=\"admin\", app=\"search\",
bs-pathname=\"/Applications/splunk/etc\"",
        "type" : "DEBUG"
      }
```

```
    ],
  "preview" : false,
  "results" : [ { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      }
    ]
}
```

POST

Access a preview of `{search_id}` search results.

Request parameters

Name	Type	Default	Description
add_summary_to_metadata	Boolean	false	Set the value to "true" to include field summary statistics in the response.
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided the union of the lists is used.
field_list	String		[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
search	String		The post processing search to apply to results. Can be any valid search language string. Only usable from POST operations.

Returned values

None

Application usage

Returns the intermediate preview results of the search specified by {search_id}. When the job is complete, this gives the same response as /search/jobs/{search_id}/results. Preview is enabled for real-time searches and for searches where status_buckets > 0.

Example request and response

JSON request

```
curl -k -u admin:pass https://localhost:8089/services/search/v2/jobs/mysearch_02151949/results_preview --get
-d f=index -d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

JSON response

```
{ "init_offset" : 0,
  "messages" : [ { "text" : "base lispy: [ AND index::_internal source::*/metrics.log ]",
        "type" : "DEBUG"
      },
      { "text" : "search context: user=\"admin\", app=\"search\",
bs-pathname=\"/Applications/splunk/etc\"",
        "type" : "DEBUG"
      }
    ],
  "preview" : false,
  "results" : [ { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      }
    ]
}
```

---

search/jobs/{search_id}/results_preview (deprecated)

```
https://<host>:<mPort>/services/search/jobs/{search_id}/results_preview
```

Preview `{search_id}` search results.

> This endpoint is deprecated as of Splunk Enterprise 9.0.1. Use the v2 instance of this endpoint instead.

GET

Preview `{search_id}` search results.

Request parameters

Name	Type	Default	Description

Name	Type	Default	Description
add_summary_to_metadata	Boolean	false	Set the value to "true" to include field summary statistics in the response.
count	Number	100	The maximum number of results to return. If value is set to `0`, then all available results are returned.
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided the union of the lists is used.
field_list	String		[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
offset	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0.
output_mode	Enum	xml	Valid values: (atom | csv | json | json_cols | json_rows | raw | xml) Specifies the format for the returned output.
search	String		The post processing search to apply to results. Can be any valid search language string.

Returned values

None

Application usage

Returns the intermediate preview results of the search specified by {search_id}. When the job is complete, this gives the same response as /search/jobs/{search_id}/results. Preview is enabled for real-time searches and for searches where status_buckets > 0.

Example request and response

JSON request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/results_preview --get -d
f=index -d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

JSON response

```
{ "init_offset" : 0,
  "messages" : [ { "text" : "base lispy: [ AND index::_internal source::*/metrics.log ]",
        "type" : "DEBUG"
      },
      { "text" : "search context: user=\"admin\", app=\"search\",
bs-pathname=\"/Applications/splunk/etc\"",
        "type" : "DEBUG"
      }
    ],
  "preview" : false,
  "results" : [ { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      },
      { "index" : "_internal",
        "source" : "/Applications/splunk/var/log/splunk/metrics.log",
        "sourcetype" : "splunkd"
      }
    ]
}
```

search/jobs/{search_id}/search.log

`https://<host>:<mPort>/services/search/jobs/{search_id}/search.log`
Get the `{search_id}` search log.

GET

Get the `{search_id}` search log.

Request parameters

Name	Type	Default	Description
attachment	Boolean	false	If true, returns search.log as an attachment. Otherwise, streams search.log.

Returned values

None

Example request and response

Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/search.log
```

Response

```
07-07-2011 21:36:22.066 INFO  ApplicationManager - Found application directory:
/Applications/splunk4.3/etc/apps/user-prefs
07-07-2011 21:36:22.066 INFO  ApplicationManager - Initialized at least 12 applications:
/Applications/splunk4.3/etc/apps
07-07-2011 21:36:22.066 INFO  ApplicationManager - Found 5 application(s) that might have global exports
07-07-2011 21:36:22.073 INFO  dispatchRunner - initing LicenseMgr in search process: nonPro=0
07-07-2011 21:36:22.074 INFO  LicenseMgr - Initing LicenseMgr
07-07-2011 21:36:22.075 INFO  ServerConfig - My GUID is "1F3A34AE-75DA-4680-B184-5BF309843919".
07-07-2011 21:36:22.075 INFO  ServerConfig - My hostname is "ombroso-mbp15.local".
07-07-2011 21:36:22.076 INFO  SSLCommon - added zlib compression
07-07-2011 21:36:22.077 INFO  ServerConfig - Default output queue for file-based input: parsingQueue.
07-07-2011 21:36:22.077 INFO  LMConfig - serverName=mbp15.splunk.com
guid=1F3A34AE-75DA-4680-B184-5BF309843919
07-07-2011 21:36:22.077 INFO  LMConfig - connection_timeout=30
07-07-2011 21:36:22.077 INFO  LMConfig - send_timeout=30
```

```
07-07-2011 21:36:22.077 INFO  LMConfig - receive_timeout=30
. . . elided . . .
```

search/jobs/{search_id}/summary

`https://<host>:<mPort>/services/search/jobs/{search_id}/summary`

Get the `getFieldsAndStats` output of the events to-date, for the `search_id` search.

GET

Get the `getFieldsAndStats` output of the events to-date, for the `search_id` search.

Request parameters

Name	Type	Default	Description
earliest_time	String		Time string representing the earliest (inclusive), respectively, time bounds for the search. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. (Also see comment for the search_mode variable.)
f	String		A field to return for the event set. You can pass multiple `POST f` arguments if multiple field are required. If `field_list` and `f` are provided, the union of the lists is used.
field_list	String		[Deprecated] Use *f*. A comma-separated list of the fields to return for the event set.
histogram	Boolean	false	Indicates whether to add histogram data to the summary output.
latest_time	String		Time string representing the latest (exclusive), respectively, time bounds for the search.
min_freq	Number	0	For each key, the fraction of results this key must occur in to be displayed. Express the fraction as a number between 0 and 1.
output_time_format	String	`time_format`	Formats a UTC time.
search	String	Empty string	Specifies a substring that all returned events should contain either in one of their values or tags.
time_format	String	%m/%d/%Y:%H:%M:%S	Expression to convert a formatted time string from {start,end}_time into UTC seconds.
top_count	Number	10	For each key, specifies how many of the most frequent items to return.

Returned values

None

Application usage

This endpoint is only valid when status_buckets > 0. To guarantee a set of fields in the summary, when creating the search, use the required_fields_list or rf parameters.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mytestsid/summary --get -d f=source -d
f=sourcetype -d f=host -d top_count=5
```

XML Response

```
<?xml version='1.0' encoding='UTF-8'?>
<summary earliest_time='1969-12-31T16:00:00.000-08:00' latest_time='1969-12-31T16:00:00.464-08:00'
duration='0' c='150375'>
  <field k='host' c='150375' nc='0' dc='1' exact='1'>
    <modes>
      <value c='150375' exact='1'><text>tiny</text></value>   </modes>
  </field>
  <field k='source' c='150375' nc='0' dc='13' exact='1'>
    <modes>
      <value c='136107' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/metrics.log</text></value>
     <value c='6682'
exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/splunkd_access.log</text></value>     <value
c='4656' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/scheduler.log</text></value>      <value
c='1714' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/web_access.log</text></value>     <value
c='937' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/splunkd.log</text></value>   </modes>
  </field>
  <field k='sourcetype' c='150375' nc='0' dc='10' exact='1'>
    <modes>
      <value c='137053' exact='1'><text>splunkd</text></value>      <value c='6682'
exact='1'><text>splunkd_access</text></value>     <value c='4656' exact='1'><text>scheduler</text></value>
     <value c='1714' exact='1'><text>splunk_web_access</text></value>      <value c='193'
exact='1'><text>splunk_web_service</text></value>    </modes>
  </field>
</summary>
```

search/jobs/{search_id}/timeline

`https://<host>:<mPort>/services/search/jobs/{search_id}/timeline`

Get event distribution over time of the untransformed events read to-date, for the `search_id` search.

GET

Get event distribution over time of the untransformed events read to-date, for the `search_id` search.

Request parameters

Name	Type	Default	Description
output_time_format	String	`time_format`	Formats a UTC time.
time_format	String	%m/%d/%Y:%H:%M:%S	Expression to convert a formatted time string from {start,end}_time into UTC seconds.

Returned values

None

The output from this endpoint provides values for the following fields:

Field	Description
c	Event count
a	Available. Not all events in a bucket are retrievable. Generally capped at 10000.
t	Time in epoch seconds
d	Bucket size (time)
f	Indicates if the search finished scanning events from the time range of this bucket.
etz	Timezone offset, in seconds, for the earliest time of this bucket. etz and ltz are different if the buckets are months or days and you have a DST change during the middle.
ltz	Timezone offset, in seconds, for the latest time of this bucket.

Application usage

This endpoint is only valid when status_buckets > 0. To guarantee a set of fields in the summary, when creating the search, use the required_fields_list or rf parameters.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mytestsid/timeline --get -d
time_format="%c"
```

XML Response

```
<timeline c='150397' cursor='1312308000'>
<bucket c='7741' a='7741' t='1312308000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 11:00:00
2011</bucket>
<bucket c='7894' a='7894' t='1312311600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 12:00:00
2011</bucket>
<bucket c='7406' a='7406' t='1312315200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 13:00:00
2011</bucket>
<bucket c='6097' a='6097' t='1312318800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 14:00:00
2011</bucket>
<bucket c='6072' a='6072' t='1312322400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 15:00:00
2011</bucket>
<bucket c='6002' a='6002' t='1312326000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 16:00:00
2011</bucket>
<bucket c='6004' a='6004' t='1312329600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 17:00:00
2011</bucket>
<bucket c='5994' a='5994' t='1312333200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 18:00:00
2011</bucket>
<bucket c='6037' a='6037' t='1312336800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 19:00:00
2011</bucket>
<bucket c='6021' a='6021' t='1312340400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 20:00:00
2011</bucket>
<bucket c='6051' a='6051' t='1312344000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 21:00:00
2011</bucket>
<bucket c='6006' a='6006' t='1312347600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 22:00:00
2011</bucket>
<bucket c='6041' a='6041' t='1312351200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 23:00:00
2011</bucket>
```

```
<bucket c='5993' a='5993' t='1312354800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 00:00:00
2011</bucket>
<bucket c='6040' a='6040' t='1312358400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 01:00:00
2011</bucket>
<bucket c='5993' a='5993' t='1312362000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 02:00:00
2011</bucket>
<bucket c='6061' a='6061' t='1312365600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 03:00:00
2011</bucket>
<bucket c='5995' a='5995' t='1312369200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 04:00:00
2011</bucket>
<bucket c='5988' a='5988' t='1312372800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 05:00:00
2011</bucket>
<bucket c='6042' a='6042' t='1312376400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 06:00:00
2011</bucket>
<bucket c='5998' a='5998' t='1312380000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 07:00:00
2011</bucket>
<bucket c='6055' a='6055' t='1312383600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 08:00:00
2011</bucket>
<bucket c='5997' a='5997' t='1312387200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 09:00:00
2011</bucket>
<bucket c='5994' a='5994' t='1312390800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 10:00:00
2011</bucket>
<bucket c='875' a='875' t='1312394400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Wed Aug  3 11:00:00
2011</bucket>
</timeline>
```

search/v2/parser

`https://<host>:<mPort>/services/search/v2/parser`

Access search language parsing.

The GET operation is not available in the v2 iteration of this endpoint.

POST

Parses Splunk search language and returns semantic map.

Request parameters

Name	Type	Default	Description
enable_lookups	Boolean	false	If `true`, reverse lookups are done to expand the search expression.
output_mode	String	xml	Specify output formatting. Select from either: xml: XML formatting json: JSON formatting
parse_only	Boolean	false	If true, disables expansion of search due evaluation of subsearches, time term expansion, lookups, tags, eventtypes, sourcetype alias.
q required	String		The search string to parse.
reload_macros	Boolean	true	If true, reload macro definitions from macros.conf.

Name	Type	Default	Description

Returned values

None

Example request and response

JSON Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/v2/parser -d output_mode=json -d
q="search index=os sourcetype=cpu"
```

JSON Response

```
{
  "remoteSearch": "litsearch  | fields  keepcolorder=t \"host\" \"index\" \"linecount\" \"source\"
\"sourcetype\" \"splunk_server\"",
  "remoteTimeOrdered": true,
  "eventsSearch": "search index=os sourcetype=cpu",
  "eventsTimeOrdered": true,
  "eventsStreaming": true,
  "reportsSearch": "",
  "commands": [
    {
      "command": "search",
      "rawargs": "",
      "pipeline": "streaming",
      "args": {
        "search": [""],
      }
      "isGenerating": true,
      "streamType": "SP_STREAM",
    },
  ]
}
```

search/parser (deprecated)

```
https://<host>:<mPort>/services/search/parser
```

Get search language parsing.

This endpoint is deprecated as of Splunk Enterprise 9.0.1. Use the v2 instance of this endpoint instead.

GET

Parses Splunk search language and returns semantic map.

Request parameters

Name	Type	Default	Description
enable_lookups	Boolean	false	If `true`, reverse lookups are done to expand the search expression.
output_mode	String	xml	Specify output formatting. Select from either: xml: XML formatting json: JSON formatting
parse_only	Boolean	false	If true, disables expansion of search due evaluation of subsearches, time term expansion, lookups, tags, eventtypes, sourcetype alias.
q required	String		The search string to parse.
reload_macros	Boolean	true	If true, reload macro definitions from macros.conf.

Returned values

None

Example request and response

JSON Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/parser --get -d
output_mode=json -d q="search index=os sourcetype=cpu"
```

JSON Response

```
{
  "remoteSearch": "litsearch  | fields  keepcolorder=t \"host\" \"index\" \"linecount\" \"source\"
\"sourcetype\" \"splunk_server\"",
  "remoteTimeOrdered": true,
  "eventsSearch": "search ",
  "eventsTimeOrdered": true,
  "eventsStreaming": true,
  "reportsSearch": "",
  "commands": [
    {
      "command": "search",
      "rawargs": "",
      "pipeline": "streaming",
      "args": {
        "search": [""],
      }
      "isGenerating": true,
      "streamType": "SP_STREAM",
    },
  ]
}
```

search/scheduler

```
https://<host>:<mPort>/services/search/scheduler
```
GET

Get current search scheduler enablement status.

Request parameters

None

Returned values

Name	Type	Default	Description
saved_searches_disabled	Boolean	0 or 1	A boolean value indicating whether the search scheduler is disabled.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/scheduler
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduler</title>
  <id>https://localhost:8089/services/search/scheduler</id>
  <updated>2015-06-09T13:23:38-07:00</updated>
  <generator build="6cfc0237739f" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/search/scheduler/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler</title>
    <id>https://localhost:8089/services/search/scheduler/scheduler</id>
    <updated>2015-06-09T13:23:38-07:00</updated>
    <link href="/services/search/scheduler/scheduler" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/scheduler/scheduler" rel="list"/>
    <link href="/services/search/scheduler/scheduler" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="saved_searches_disabled">0</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

search/scheduler/status

```
https://<host>:<mPort>/services/search/scheduler/status
```

Enable or disable the search scheduler.

POST

Enable or disable the search scheduler.

Request parameters

Name	Type	Default	Description
disabled	Boolean		Indicates whether to disable the search scheduler. 0 enables the search scheduler. 1 disables the search scheduler.

Returned values

None

Example request and response

XML Request

```
curl -ku admin:pass -XPOST https://localhost:8089/services/search/scheduler/status -d disabled=1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduler</title>
  <id>https://localhost:8089/services/search/scheduler</id>
  <updated>2015-06-09T13:40:21-07:00</updated>
  <generator build="6cfc0237739f" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/search/scheduler/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

search/timeparser

`https://<host>:<mPort>/services/search/timeparser`
Get time argument parsing.

GET

Get a lookup table of time arguments to absolute timestamps.

Request parameters

Name	Type	Default	Description
now	String		The time to use as current time for relative time identifiers. Can itself either be a relative time (from the real "now" time) or an absolute time in the format specified by `time_format`.
output_time_format	String	%FT%T.%Q%:z	Used to format a UTC time. Defaults to the value of `time_format`.
time required	String		The time argument to parse. Acceptable inputs are either a relative time identifier or an absolute time. Multiple time arguments can be passed by specifying multiple time parameters.
time_format	String	%FT%T.%Q%:z	The format (`strftime`) of the absolute time format passed in time. This field is not used if a relative time identifier is provided. For absolute times, the default value is the ISO-8601 format.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/timeparser --get -d time=-12h -d
time=-24h
```

XML Response

```
<response>
  <dict>
    <key name="-12h">2011-07-06T21:54:23.000-07:00</key>
    <key name="-24h">2011-07-06T09:54:23.000-07:00</key>
  </dict>
</response>
```

search/typeahead

`https://<host>:<mPort>/services/search/typeahead`

Get search string auto-complete suggestions.

GET

Get a list of words or descriptions for possible auto-complete terms.

Request parameters

Name	Type	Default	Description
count required	Number		The number of items to return for this term.
max_servers	Number	2	Specifies the maximum number of indexer search peers that are used in addition to the search head for the purpose of providing typeahead functionality. When properly set, `max_servers` minimizes the workload impact of running typeahead search jobs in an indexer clustering deployment. If your target indexes are evenly distributed among search servers, use the default setting or a similarly low number. For load balancing, the choice of search peers for typeahead searches is random. A setting of `0` means "no limit": All available search peers are used for `typeahead` search jobs.
output_mode	String	csv	Specify output formatting. Select from: csv: CSV formatting xml: XML formatting json: JSON formatting
prefix required	String		The term for which to return typeahead results.

Returned values

None

Example request and response

JSON Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/typeahead --get -d count=3 -d
prefix=source -d output_mode=json max_servers=1
```

JSON Response

```
{ "results" : [ { "content" : "source=\"sampledata.zip:./apache1.splunk.com/access_combined.log\"",
        "count" : 9199,
        "operator" : false
      },
      { "content" : "source=\"sampledata.zip:./apache2.splunk.com/access_combined.log\"",
        "count" : 27705,
        "operator" : false
      },
      { "content" : "source=\"sampledata.zip:./apache3.splunk.com/access_combined.log\"",
        "count" : 27888,
        "operator" : false
      }
    ]
}
```

Endpoints for SPL2-based applications

This documentation is designed for Splunk application developers and Splunk administrators who are creating or managing SPL2-based applications. For more information see:

- Create SPL2-based apps in the *Splunk Developer Guide* on dev.splunk.com.
- **Splunk Enterprise**: Install SPL2-based apps in the *Splunk Enterprise Admin Manual*.
- **Splunk Cloud Platform**: Install SPL2-based apps in the *Splunk Cloud Platform Admin Manual*.

search/spl2-module-dispatch

```
https://<host>:<mport>/services/search/spl2-module-dispatch
```

Dispatch a module containing one or more SPL2 statements. For more information about what constitutes an SPL2 statement, see Modules and SPL2 statements in the *SPL2 Search Manual*.

POST

Start a new search or searches and return a search ID (SID) for each named search statement.

Request parameters

Name	Type	Default	Description
module	String		**Required.** Contains the entire module definition including imports, within quotation marks. Example: `import _internal from ../../../../indexes;$query_name = FROM _internal`
namespace	String		The application namespace in which to restrict searches. Leave blank with only quotation marks. Example: " "

Name	Type	Default	Description
queryParameters	String		**Required.** Contains a list of searches by name. Each search requires its own queryName and associated metadata, and returns a separate SID.
queryName	String		**Required.** The name of each search in the query, followed by a stanza containing its associated metadata. You must separately specify each search in the module, or your request will not return results for that search.
earliest	String	-24h@h	A time string that specifies the earliest time to retrieve events. Can be a relative or absolute time. For absolute time, specify either UNIX time or UTC in seconds in the ISO-8601 (`%FT%T.%Q`) format. To learn about time strings in SPL2, see Time modifiers in the *SPL2 Search Manual*. Example: `2019-01-25T13:15:30Z`.
latest	String	now	A time string that specifies the latest time to retrieve events. Can be a relative or absolute time. For absolute time, specify either UNIX time or UTC in seconds in the ISO-8601 (`%FT%T.%Q`) format. To learn about time strings in SPL2, see Time modifiers in the *SPL2 Search Manual*. Example: `2019-01-25T13:15:30Z`.
timezone	String	Current system timezone	Specifies the timezone for the earliest and latest parameters, if those parameters are in relative time. If those parameters are in absolute time, then this parameter is ignored. Specify time zone for timestamps. To see all supported time zone formats, see Time zones.
relativeTimeAnchor	String	The time the search job is created	Specifies the anchor time for the earliest and latest parameters, if those parameters are in relative time. Example: If earliest is set to `-d@d`, the unit is day. If the relativeTimeAnchor is set to `2020-10-05T13:15:30Z`, then resolvedEarliest becomes `2020-10-05T00:00:00Z`, which is the day. Hours, minutes, and seconds are set to zero.
collectEventSummary	Boolean	False	Specifies whether a search can collect event summary information during the run time.
collectFieldSummary	Boolean	False	Specifies whether a search can collect fields summary information during the run time.
collectTimeBuckets	Boolean	False	Specifies whether a search can collect timeline buckets summary information during the run time.
adhocSearchLevel	String	fast	Specify the mode in which the search should run. Accepts `fast`, `smart`, or `verbose`.

Returned values

Name	Description
sid	Search ID.
name	Name of the search statement.

Example request

```
curl -k -u <admin>:<changeme> --location 'https://<host>:8089/services/search/spl2-module-dispatch' \
--data '{
  "module": " $search1 = from _audit | stats count()",
  "namespace": "",
  "queryParameters": {
   "search1": {
            "earliest": "-1h@h",
            "latest": "now",
            "timezone": "Etc/UTC",
            "collectFieldSummary": true
    }
   "search2": {
            "earliest": "-1h@h",
            "timezone": "Etc/UTC",
            "collectEventSummary": true
    }
  }
}'
```

Example response

```
[
    {
        "sid": "1682980180.52",
        "name": "search1"
    }
{
        "sid": "1058392067.22",
        "name": "search2"
    }
]
```

services/spl2/modules

```
https://<host>:<mport>/services/spl2/modules
```

Access a list of SPL2 modules.

POST

Create a module within the app context.

Request parameters

Name	Type	Default	Description
module	String		**Required.** The name of the module.
namespace	String		**Required.** The namespace of the module.
definition	String		**Required.** The definition of the module. Example: `"$a = | FROM index:terminallookup4704 GROUP BY indexed:source SELECT count();"`

Returned values None.

Example request

```
curl -k --request POST -u admin:pass 'https://localhost:8089/services/spl2/modules' \
--data-raw '{
    "name": "bar",
    "namespace": "foo",
    "definition": "$a = | FROM index:terminallookup4704 GROUP BY indexed:source      SELECT count();"
}'
```

Example response

See HTTP Status Codes for a list of possible responses.

services/spl2/modules/{resourceName}

```
https://<host>:<mport>/services/spl2/modules/{resourceName}
```

Access a specific SPL2 module.

GET

Retrieves information about a specific module.

Request parameters None.

Example request

```
curl -k -u admin:pass https://localhost:8089/services/spl2/modules/foo.bar
```

Example response

```
{
 "namespace": "apps.sample_app_spl2",
 "name": "_default",
 "definition": "$a = | FROM _internal | limit 10 ;export $a;",
 "createdAt": "2023-08-03T00:17:31Z",
 "createdBy": "admin",
 "updatedAt": "2023-08-03T00:17:31Z",
 "updatedBy": "admin"
}
```

PUT

Create or update a specific module within the app context.

Request parameters

Name	Type	Default	Description
namespace	String		**Required.** The namespace of the module.
definition	String		**Required.** The definition of the module. Example: `"$a = | FROM index:terminallookup4704 GROUP BY indexed:source SELECT count();"`

Example request

```
curl -k --request POST -u admin:pass 'https://localhost:8089/services/spl2/modules/foo.bar' \
--data-raw '{
    "name": "bar",
    "namespace": "foo",
    "definition": "$a = | FROM index:terminallookup4704 GROUP BY indexed:source      SELECT count();"
}'
```

Example response See HTTP Status Codes for a list of possible responses. In addition to one of the listed responses, this endpoint might also return the following additional status code:

HTTP status code	Description
415	Unsupported media type. The type must be `application/json`.

DELETE

Delete a specific module within the app context.

Request parameters None.

Example request

```
curl -k -u admin:pass -X "DELETE" https://localhost:8089/services/spl2/modules/search.module.testmodule
```

Example response

```
{
    "code": "not_found",
    "message": "Module does not exist/already deleted"
}
```

See HTTP Status Codes for a list of possible responses.

services/spl2/permissions

```
https://<host>:<mport>/services/spl2/permissions
```

Access a list of role-based permissions for a module. Requires the edit_spl2_permissions capability.

POST

Update permissions for a module.

Request parameters

Name	Type	Default	Description
resourceType	String		**Required.** Must be either "modules" or "views".
resourceName	String	All objects	**Required.** Name of a specific module or view.
permissions	JSON array		**Required.** Array containing permissions for each type of supported operation.

Returned values

See HTTP Status Codes for a list of possible responses.

Example request

```
curl -k -u admin:pass https://localhost:8089/services/spl2/permissions \
--data '{
  "resourceType": "modules",
  "resourceName": "module1",
  "permissions": [
    {
      "operation": "read",
      "roles": [
        "admin",
        "user",
        "editor"
      ]
    },
    {
      "operation": "write",
      "roles": [
        "editor"
      ]
    }
  ]
}'
```

Example response

```
{
   "code":201
}
```

services/spl2/permissions/role/{rolename}

```
https://<host>:<mport>/services/spl2/permissions/role/{rolename}
```

Access a list of all permissions for a given role. Requires the edit_spl2_permissions capability.

GET

Get all permissions for a given role.

Request parameters

None.

Example request

```
curl -k -u admin:pass https://localhost:8089/services/spl2/permissions/role/editor
```

Example response

```
[{
  "resourceType": "",
  "resourceName": "",
  "permissions": [
    {
      "operation": "read",
      "roles": [
        "admin",
        "user",
        "editor"
      ]
    },
    {
      "operation": "write",
      "roles": [
        "editor"
      ]
    }
  ]
}]
```

services/spl2/permissions/user/{username}

```
https://<host>:<mport>/services/spl2/permissions/user/{username}
```

Access a list of all permissions for a given user. Requires the edit_spl2_permissions capability.

GET

Get all permissions for a given user.

Request parameters

None.

Example request

```
curl -k -u admin:pass https://localhost:8089/services/spl2/permissions/user/user1
```

Example response

```
{
  "resourceType": "",
  "resourceName": "",
  "permissions": [
    {
      "operation": "read",
      "roles": [
        "admin",
        "user",
        "editor"
      ]
    },
    {
      "operation": "write",
      "roles": [
        "editor"
      ]
    }
  ]
}
```

System endpoints

System endpoint descriptions

Manage server configuration settings and messages.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Additional introspection information

See Introspection endpoint descriptions for the system endpoints related to introspection.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. System endpoints are generally not accessible in Splunk Cloud Platform.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

---

messages

```
https://<host>:<mPort>/services/messages
```

Access and create system messages. Most messages are created by splunkd to inform the user of system information, including license quotas, license expirations, misconfigured indexes, and disk space. Splunk Web displays these as bulletin board messages.

GET

Show systemwide messages.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys
Depending on the system status, messages returned vary. Messages returned in the response include a name and description, as in the following example.

Name	Description
help	For internal use only
<message_name>	The message name depends on the specific message returned. This field might contain the same text as the *message* field. In the following example response, this field is `"manifest_error"`.
message	Message text
server	Name of the server that generated the error
severity	One of the following message severity values • `info` • `warn` • `error`
timeCreated_epochSecs	Timestamp when the message was posted
timeCreated_iso	ISO formatted timestamp

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/messages
```

XML Response

```
<title>messages</title>
  <id>https://10.140.53.114:8089/services/admin/messages</id>
     ...
  <entry>
    <title>manifest_error</title>
    <id>https://10.140.53.114:8089/services/admin/messages/manifest_error</id>
    <updated>2016-09-01T13:10:34-07:00</updated>
    <link href="/services/admin/messages/manifest_error" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/messages/manifest_error" rel="remove"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="help"></s:key>
        <s:key name="manifest_error">File Integrity checks found 145 files that did not match the
system-provided manifest.  See splunkd.log for details.</s:key>
        <s:key name="message">File Integrity checks found 145 files that did not match the system-provided
manifest.  See splunkd.log for details.</s:key>
        <s:key name="server">docs-unix-4</s:key>
        <s:key name="severity">warn</s:key>
        <s:key name="timeCreated_epochSecs">1472739529</s:key>
        <s:key name="timeCreated_iso">2016-09-01T07:18:49-07:00</s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Create a persistent message displayed at /services/messages.

Request parameters

Name	Type	Description
<name>	String	**Required**. Message name (key).
capability	String	One or more capabilities that users must have to view the message. Capability names are validated. If multiple capabilities are required, include them each as separate fields.
role	Comma separated list	One or more roles that users must have to view the message. Role names are validated.
value	String	**Required**. Message text.
severity	String	One of the following message severity values. • `info` • `warn` • `error`

Name	Type	Description

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/messages -d name=helloMessage -d value="hello
world" -d severity="info"
```

XML Response

```
.
.
.
<title>messages</title>
 <id>https://localhost:8089/services/messages</id>
 <updated>2014-02-20T10:24:02-08:00</updated>
 <generator build="197187" version="6.1beta"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/messages/_new" rel="create"/>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>helloMessage</title>
   <id>https://localhost:8089/services/messages/helloMessage</id>
   <updated>2014-02-20T10:24:02-08:00</updated>
   <link href="/services/messages/helloMessage" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/messages/helloMessage" rel="remove"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="helloMessage">"hello world"</s:key>
       <s:key name="eai:acl">
          ... elided ...
       </s:key>
       <s:key name="message">"hello world"</s:key>
       <s:key name="severity">info</s:key>
       <s:key name="timeCreated_epochSecs">1392920642</s:key>
     </s:dict>
   </content>
 </entry>
```

messages/{name}

```
https://<host>:<mPort>/services/messages/{name}
```

Manage the message associated with the `{name}` message ID.

DELETE

Delete the specified message.

Request parameters
None

Response keys
None. An HTTP status code = `500` is returned if `{name}` message does not exist.

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/messages/message
```

XML Response

```
.
.
.
 <title>messages</title>
 <id>https://localhost:8089/services/messages</id>
 <updated>2011-07-08T01:14:21-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/messages/_new" rel="create"/>
    ... opensearch elements elided ...
 <s:messages/>
```

GET

Get details of the specified message.

Request parameters
None

Response keys

Name	Description
help	For internal use only
<message_name>	The message name depends on the specific message returned. This field might contain the same text as the *message* field. In the following example response, this field is "`manifest_error`".
message	Message text
server	Name of the server that generated the error

Name	Description
severity	One of the following message severity values • `info` • `warn` • `error`
timeCreated_epochSecs	Timestamp when the message was posted
timeCreated_iso	ISO formatted timestamp

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/messages/manifest_error
```

XML Response

```
...
<title>messages</title>
  <id>https://localhost:8089/services/admin/messages</id>
  <updated>2016-09-01T13:10:59-07:00</updated>
  <generator build="3b17605ee8e3" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/messages/_new" rel="create"/>
  <link href="/services/admin/messages/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>manifest_error</title>
    <id>https://localhost:8089/services/admin/messages/manifest_error</id>
    <updated>2016-09-01T13:10:59-07:00</updated>
    <link href="/services/admin/messages/manifest_error" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/messages/manifest_error" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list/>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="help"></s:key>
        <s:key name="manifest_error">File Integrity checks found 145 files that did not match the
system-provided manifest.  See splunkd.log for details.</s:key>
        <s:key name="message">File Integrity checks found 145 files that did not match the system-provided
manifest.  See splunkd.log for details.</s:key>
        <s:key name="server">docs-unix-4</s:key>
        <s:key name="severity">warn</s:key>
        <s:key name="timeCreated_epochSecs">1472739529</s:key>
        <s:key name="timeCreated_iso">2016-09-01T07:18:49-07:00</s:key>
      </s:dict>
    </content>
  </entry>
```

server/control

`https://<host>:<mPort>/services/server/control`

List available controls.

GET

List actions that can be performed at this endpoint.

Request parameters

None

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/control
```

XML Response

```
.
.
.
 <title>server-control</title>
 <id>https://localhost:8089/services/server/control</id>
 <updated>2011-07-12T00:17:53-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/server/control/restart" rel="restart"/>
    ... opensearch elements elided ...
 <s:messages/>
```

server/control/restart

`https://<host>:<mPort>/services/server/control/restart`

Restart the splunkd server daemon and Splunk Web interface. The POST operation is equivalent to the `splunk restart` CLI command.

See also server/control/restart_webui

POST

Restart the splunkd server daemon and Splunk Web interface.

Request parameters

None

Response keys

An HTTP status code `200` indicates successful restart.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/control/restart -X POST
```

XML Response

```
.
.
```

```
.
 <title>server-control</title>
 <id>https://localhost:8089/services/server/control</id>
 <updated>2014-08-05T13:02:50-07:00</updated>
 <generator build="221120" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/server/control/restart" rel="restart"/>
 <link href="/services/server/control/restart_webui" rel="restart_webui"/>
 ... opensearch nodes elided ...
 <s:messages/>
```

server/control/restart_webui

```
https://<host>:<mPort>/services/server/control/restart_webui
```

Restart the Splunk Web interface. This interface is equivalent to the `splunk restart splunkweb` CLI command, and restarts the Web interface on servers with the default app server mode set. See also server/control/restart

POST

Restart the Splunk Web interface.

Request parameters

None

Response keys

An HTTP status code `200` indicates successful restart.

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/control/restart_webui -X POST
```

XML Response

```
.
.
.
 <title>server-control</title>
 <id>https://localhost:8089/services/server/control</id>
 <updated>2014-08-05T12:10:37-07:00</updated>
 <generator build="221120" version="6.2"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/server/control/restart" rel="restart"/>
 <link href="/services/server/control/restart_webui" rel="restart_webui"/>
```

```
... opensearch elements elided ...
<s:messages/>
```

server/httpsettings/proxysettings

`https://<host>:<mPort>/services/server/httpsettings/proxysettings`
Create an HTTP Proxy Server configuration for splunkd.

Authentication and Authorization
Requires the `edit_server` capability.

POST

Create a HTTP Proxy server configuration stanza for use with splunkd.

The POST request generates a `proxyConfig` configuration that you can access or update at `server/settings/httpsettings/proxysettings/proxyConfig`.

Request parameters

Name	Type	Description
name	String	**Required**. Use "`proxyConfig`" to name the configuration stanza.

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/httpsettings/proxysettings -d
name="proxyConfig''
```

XML Response

```
<entry>
   <title>proxyConfig</title>
   <id>https://localhost:8089/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig</id>
   <updated>1969-12-31T16:00:00-08:00</updated>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="alternate"/>
   <author>
     <name>nobody</name>
   </author>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="list"/>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/_reload"
rel="_reload"/>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="edit"/>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="remove"/>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/move" rel="move"/>
   <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/disable"
```

```
rel="disable"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="disabled">0</s:key>
       <s:key name="eai:acl">
         <s:dict>
           <s:key name="app">search</s:key>
           <s:key name="can_change_perms">1</s:key>
           <s:key name="can_list">1</s:key>
           <s:key name="can_share_app">1</s:key>
           <s:key name="can_share_global">1</s:key>
           <s:key name="can_share_user">0</s:key>
           <s:key name="can_write">1</s:key>
           <s:key name="modifiable">1</s:key>
           <s:key name="owner">nobody</s:key>
           <s:key name="perms">
             <s:dict>
               <s:key name="read">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
               <s:key name="write">
                 <s:list>
                   <s:item>*</s:item>
                 </s:list>
               </s:key>
             </s:dict>
           </s:key>
           <s:key name="removable">1</s:key>
           <s:key name="sharing">app</s:key>
         </s:dict>
       </s:key>
     </s:dict>
   </content>
 </entry>
```

server/httpsettings/proxysettings/proxyConfig

`https://<host>:<mPort>/services/server/httpsettings/proxysettings/proxyConfig`
Access, update, or delete the HTTP Proxy Server configurations for splunkd including `http_proxy`, `https_proxy` and `no_proxy`.

Authentication and Authorization

All operations on this endpoint require the `edit_server` capability.

GET

Access the `{proxyConfig}` HTTP proxy server configurations for splunkd.

Request parameters

Name	Type	Description

http_proxy	String	Identifies the server proxy. When set, splunkd sends all HTTP requests through the proxy server defined in `http_proxy` on the proxy. The default value is unset.
https_proxy	String	Identifies the server proxy. When set, splunkd sends all HTTPS requests through the proxy server defined in `https_proxy`. If not set, splunkd uses the `http_proxy` variable instead. The default value is unset.
no_proxy	String	Identifies the no proxy rules. When set, splunkd uses these rules to decide whether the proxy server needs to be bypassed for matching hosts and IP addresses. Requests going to a `localhost/loopback` address are not proxied. The default value is `localhost, 127.0.0.1, ::1`.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/server/httpsettings/proxysettings -d
name="proxyConfig''
```

XML Response

```
  <entry>
    <title>proxyConfig</title>
    <id>https://localhost:8089/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="list"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="edit"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="remove"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/move" rel="move"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>http_proxy</s:item>
                <s:item>https_proxy</s:item>
                <s:item>no_proxy</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
```

POST

Update the `{proxyConfig}` HTTP proxy server configurations for splunkd.

Request parameters

Name	Type	Description
http_proxy	String	Identifies the server proxy. When set, splunkd sends all HTTP requests through the proxy server defined in `http_proxy` on the proxy. The default value is unset.
https_proxy	String	Identifies the server proxy. When set, splunkd sends all HTTPS requests through the proxy server defined in `https_proxy`. If not set, splunkd uses the `http_proxy` variable instead. The default value is unset.
no_proxy	String	Identifies the no proxy rules. When set, splunkd uses these rules to decide whether the proxy server needs to be bypassed for matching hosts and IP addresses. Requests going to a `localhost/loopback` address are not proxied. The default value is `localhost, 127.0.0.1, ::1`.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/server/httpsettings/proxysettings -d
no_proxy="test''
```

XML Response

```
  <entry>
    <title>proxyConfig</title>
    <id>https://localhost:8089/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="list"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/_reload"
rel="_reload"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="edit"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="remove"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/move" rel="move"/>
    <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/disable"
rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="no_proxy">test</s:key>
      </s:dict>
    </content>
  </entry>
```

DELETE

Delete the `{proxyConfig}` HTTP proxy server configurations for splunkd.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/server/httpsettings/proxysettings/proxyConfig -X
DELETE
```

XML Response

```
<title>proxysettings</title>
  <id>https://wimpy.sv.splunk.com:34001/services/server/httpsettings/proxysettings</id>
  <updated>2017-04-20T17:14:52-07:00</updated>
  <generator build="845bc99189da" version="6.6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/httpsettings/proxysettings/_new" rel="create"/>
  <link href="/services/server/httpsettings/proxysettings/_reload" rel="_reload"/>
  <link href="/services/server/httpsettings/proxysettings/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
```

server/logger

```
https://<host>:<mPort>/services/server/logger
```

Access `splunkd` logging categories specified in code or in `$SPLUNK_HOME/etc/log.cfg`.

GET

Enumerate splunkd logging categories.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

Name	Description
level	One of the following valid logger levels for this server. • FATAL • WARN • INFO • DEBUG

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/logger
```

XML Response

```
.
.
.
<title>logger</title>
 <id>https://mrt:8089/services/server/logger</id>
 <updated>2011-05-16T20:29:38-0700</updated>
 <generator version="98144"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>AdminHandler:AuthenticationHandler</title>
   <id>https://mrt:8089/services/server/logger/AdminHandler%3AAuthenticationHandler</id>
   <updated>2011-05-16T20:29:38-0700</updated>
   <link href="/services/server/logger/AdminHandler%3AAuthenticationHandler" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/logger/AdminHandler%3AAuthenticationHandler" rel="list"/>
   <link href="/services/server/logger/AdminHandler%3AAuthenticationHandler" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">... elided ...</s:key>
       <s:key name="level">WARN</s:key>
     </s:dict>
   </content>
 </entry>
       .
       .
       .
     elided
       .
       .
       .
 <entry>
   <title>Application</title>
   <id>https://mrt:8089/services/server/logger/Application</id>
   <updated>2011-05-16T20:29:38-0700</updated>
   <link href="/services/server/logger/Application" rel="alternate"/>
```

```
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/logger/Application" rel="list"/>
  <link href="/services/server/logger/Application" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">... elided ...</s:key>
      <s:key name="level">WARN</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>ApplicationManager</title>
  <id>https://mrt:8089/services/server/logger/ApplicationManager</id>
  <updated>2011-05-16T20:29:38-0700</updated>
  <link href="/services/server/logger/ApplicationManager" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/logger/ApplicationManager" rel="list"/>
  <link href="/services/server/logger/ApplicationManager" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">... elided ...</s:key>
      <s:key name="level">WARN</s:key>
    </s:dict>
  </content>
</entry>
```

server/logger/{name}

`https://<host>:<mPort>/services/server/logger/{name}`

Manage the `{name}` logging category.

GET

Access information about the specified splunkd logging category.

Request parameters

None

Response keys

Name	Description
level	One of the following valid logger levels for this server. • FATAL • WARN • INFO • DEBUG

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/logger/Application
```

XML Response

```
.
.
.
<title>logger</title>
 <id>https://localhost:8089/services/server/logger</id>
 <updated>2011-07-02T15:10:44-07:00</updated>
 <generator version="100492"/>
 <author>
   <name>Splunk</name>
 </author>
    ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>Application</title>
   <id>https://localhost:8089/services/server/logger/Application</id>
   <updated>2011-07-02T15:10:44-07:00</updated>
   <link href="/services/server/logger/Application" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/logger/Application" rel="list"/>
   <link href="/services/server/logger/Application" rel="edit"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">... elided ...</s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list/>
           </s:key>
           <s:key name="requiredFields">
             <s:list>
               <s:item>level</s:item>
             </s:list>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="level">WARN</s:key>
     </s:dict>
   </content>
 </entry>
```

POST

Set the logging level for a specific logging category.

Request parameters

Name	Type	Description
level	Enum	**Required**. The desired logging level for this category. One of the following valid values. [FATAL | WARN | INFO | DEBUG]

Response keys

None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/logger/Application -d level=INFO
```

XML Response

```
.
.
.
 <title>logger</title>
 <id>https://localhost:8089/services/server/logger</id>
 <updated>2011-07-07T00:24:02-07:00</updated>
 <generator version="102807"/>
 <author>
   <name>Splunk</name>
 </author>
 <s:messages/>
```

server/roles

```
https://<host>:<mPort>/services/server/roles
```

Access server role information.

See also the `server-roles` attribute in /server/info.

GET

Access the roles applicable to this server.

Request parameters

None

Response keys

Name	Description

Name	Description
<variable>	Zero or more of the following possible server roles. • indexer • universal_forwarder • heavyweight_forwarder • lightweight_forwarder • license_master • license_slave • cluster_master • cluster_slave • cluster_search_head • deployment_server • deployment_client • search_head • search_peer • shc_captain • shc_deployer • shc_member

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/roles
```

XML Response

```
.
.
.
 <title>server-roles</title>
 <id>https://localhost:8089/services/server/roles</id>
 <updated>2014-04-02T12:13:07-07:00</updated>
 <generator build="200839" version="6.1"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/server/roles/catalog_allPossible_predefined" rel="catalog_allPossible_predefined"/>
   ... opensearch elements elided ...
 <s:messages/>
 <entry>
   <title>result</title>
   <id>https://localhost:8089/services/server/roles/result</id>
   <updated>2014-04-02T12:13:07-07:00</updated>
   <link href="/services/server/roles/result" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/server/roles/result" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="eai:acl">
           ... elided ...
       </s:key>
       <s:key name="indexer"/>
       <s:key name="license_master"/>
       <s:key name="license_slave"/>
```

```
    </s:dict>
  </content>
</entry>
```

server/security/rotate-splunk-secret

```
https://<host>:<mPort>/services/server/security/rotate-splunk-secret
```

Rotates the `splunk.secret` file on a standalone Splunk Enterprise instance.

POST

Rotates the `splunk.secret` file on a standalone Splunk Enterprise instance.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changeme  https://localhost:8089/services/server/security/rotate-splunk-secret -X POST
```

XML Response

server/settings

```
https://<host>:<mPort>/services/server/settings
```

Access server configuration information for a Splunk platform instance. For additional information about your Splunk platform instance, see the server/info endpoint.

GET

Returns server configuration for a Splunk deployment.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Name	Description

Name	Description
SPLUNK_DB	Absolute filepath to the default index for this deployment.
SPLUNK_HOME	Absolute filepath to the local installation of this deployment.
enableSplunkWebSSL	Indicates if HTTPS and SSL are enabled for Splunk Web.
host	The default hostname to use for data inputs that do not override this setting.
httpport	Port on which Splunk Web listens for this instance. Defaults to 8000. If using SSL, set to the HTTPS port number.
mgmtHostPort	The port on which Splunk Web listens for management operations. Defaults to 8089.
minFreeSpace	Safe amount of space in MB that must exist for splunkd to continue operating. `minFreespace` affects search and indexing in the following ways. • Before attempting to launch a search, the Splunk platform requires this amount of free space on the filesystem where the dispatch directory is stored, `$SPLUNK_HOME/var/run/splunk/dispatch`. • Applied similarly to the search quota values in authorize.conf and limits.conf. • For indexing, periodically, the indexer checks space on all partitions that contain splunk indexes as specified by indexes.conf. When you need to clear more disk space, indexing is paused and the Splunk platform posts a UI banner + warning.
pass4SymmKey	Password string prefixed to the Splunk platform symmetric key, generating the final key to sign all traffic between master/slave licenser.
serverName	Name identifying this instance for features such as distributed search.
sessionTimeout	Time range string to indicate the amount of time before a user session times out. Expressed as a search-like time range. The default is 1h (one hour). Here are some examples. `24h` (24 hours) `3d` (3 days) `7200s` (7200 seconds, or two hours)
startwebserver	Indicates whether Splunk Web is configured to start by default.
trustedIP	IP address of the authenticating proxy. Set to a valid IP address to enable SSO. Disabled by default. Normal value is '127.0.0.1'

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/settings
```

XML Response

```
.
.
.
<title>server-settings</title>
 <id>https://localhost:8089/services/server/settings</id>
 <updated>2011-07-08T01:56:40-07:00</updated>
```

```
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
   ... opensearch elements elided ...
<s:messages/>
<entry>
  <title>settings</title>
  <id>https://localhost:8089/services/server/settings/settings</id>
  <updated>2011-07-08T01:56:40-07:00</updated>
  <link href="/services/server/settings/settings" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/settings/settings" rel="list"/>
  <link href="/services/server/settings/settings" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="SPLUNK_DB">/home/amrit/temp/curl/splunk/var/lib/splunk</s:key>
      <s:key name="SPLUNK_HOME">/home/amrit/temp/curl/splunk</s:key>
      ... eai:acl node elided ...
      <s:key name="enableSplunkWebSSL">0</s:key>
      <s:key name="host">MrT</s:key>
      <s:key name="httpport">8001</s:key>
      <s:key name="mgmtHostPort">8085</s:key>
      <s:key name="minFreeSpace">2000000</s:key>
      <s:key name="pass4SymmKey">changeme</s:key>
      <s:key name="serverName">MrT</s:key>
      <s:key name="sessionTimeout">1h</s:key>
      <s:key name="startwebserver">1</s:key>
      <s:key name="trustedIP"/>
    </s:dict>
  </content>
</entry>
```

Workload management endpoints

Workload management endpoint descriptions

Manage system resources for search and indexing processes.

- Create workload pools (CPU and memory resource groups).
- Create workload rules to grant access and prioritize workload pools.
- Assign scheduled and ad hoc searches to workload pools.

For more information, see About workload management in the *Workload Management* manual.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings** > **Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings** > **Access controls** and click **Roles**.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

Splunk Cloud Platform limitations

As a Splunk Cloud Platform user, you are restricted to interacting with the search tier only with the REST API. Workload management endpoints are generally not accessible in Splunk Cloud Platform.

See Access requirements and limitations for the Splunk Cloud Platform REST API in the the *REST API Tutorials* manual for more information.

workloads/categories

```
https://<host>:<mPort>/services/workloads/categories
```

List and edit workload categories.

There are three predefined categories: search, ingest, and misc. You cannot create or delete categories. You can only edit and list them.

Authentication and Authorization

- GET requires the `list_workload_pools` capability.
- POST requires the `edit_workload_pools` capability.

GET

List information about workload categories.

Request parameters

None

Returned values

Name	Type	Description
cpu_weight	Number	Specifies the fraction of the cpu assigned to this category as a ratio of the total of cpu_weight across all categories. This fraction is then applied to the cpu shares assigned to the parent group. The value must be > 0 and <= 100.
mem_weight	Number	Specifies the percentage of memory assigned to this category as a percent of the parent group. The total amount of memory limit for this category is a percentage of the value assigned to the parent group. The value must be > 0 and <= 100.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/categories/search
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-categories</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/categories</id>
  <updated>2019-03-20T14:11:59-07:00</updated>
  <generator build="8c85c1fbcc8c" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/categories/_reload" rel="_reload"/>
  <link href="/services/workloads/categories/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/system/workloads/categories/search</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/system/workloads/categories/search" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/workloads/categories/search" rel="list"/>
    <link href="/servicesNS/nobody/system/workloads/categories/search/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/workloads/categories/search" rel="edit"/>
    <link href="/servicesNS/nobody/system/workloads/categories/search/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="cpu_allocated_percent">70.00</s:key>
        <s:key name="cpu_weight">70</s:key>
        <s:key name="cpu_weight_sum">100</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>cpu_weight</s:item>
                <s:item>mem_weight</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="mem_allocated_percent">60.00</s:key>
        <s:key name="mem_weight">60</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Edit workload categories.

Request parameters

Name	Type	Description
cpu_weight	Number	Specifies the fraction of the cpu assigned to this category as a ratio of the total of cpu_weight across all categories. This fraction is then applied to the cpu shares assigned to the parent group. The value must be > 0 and <= 100
mem_weight	Number	Specifies the percentage of memory assigned to this pool as a percent of the parent group. The total amount of memory limit for this pool is a percentage of the value assigned to the parent group. The value must be > 0 and <= 100.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/categories/search -d cpu_weight=40 -d
mem_weight=50
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-categories</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/categories</id>
  <updated>2019-03-20T14:21:44-07:00</updated>
  <generator build="8c85c1fbcc8c" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/categories/_reload" rel="_reload"/>
  <link href="/services/workloads/categories/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search</title>
    <id>https://localhost:8089/servicesNS/nobody/search/workloads/categories/search</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/workloads/categories/search" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/workloads/categories/search" rel="list"/>
    <link href="/servicesNS/nobody/search/workloads/categories/search/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/workloads/categories/search" rel="edit"/>
    <link href="/servicesNS/nobody/search/workloads/categories/search/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
```

```
        <s:key name="cpu_allocated_percent">57.14</s:key>
        <s:key name="cpu_weight">40</s:key>
        <s:key name="cpu_weight_sum">70</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="mem_allocated_percent">60.00</s:key>
        <s:key name="mem_weight">60</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

workloads/pools

`https://<host>:<mPort>/services/workloads/pools`
Perform CRUD operations on workload pools.

Authentication and Authorization

- GET requires the `list_workload_pools` capability.
- POST and DELETE require the `edit_workload_pools` capability.

GET

List information about workload pools.

Request parameters

None

Returned values

Name	Type	Description
cpu_weight	Number	Specifies the fraction of the cpu assigned to this pool as a ratio of the total of cpu_weight across all pools in a category. This fraction is then applied to the cpu shares assigned to the category.
mem_weight	Number	Specifies the amount of memory assigned to this pool as a percent of the value assigned to the category.
category	string	Specifies the category in which a poll is created. Can be either "search", "ingest", or "misc".
default_category_pool	Boolean	Specifies the workload pool marked as default pool for its category. This property is defined per workload_pool stanza. Default is 0.
default_pool	Boolean	Specifies a workload pool defined in the search category as the default pool for the search category. **Note:** deprecated parameter retained for backwards compatibility with 7.2.x
ingest_pool	Boolean	Specifies a workload-pool defined in the ingest category as the default pool for the ingest category. **Note:** deprecated parameter retained for backwards compatibility with 7.2.x

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/pools/search_pool_1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-pools</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/pools</id>
  <updated>2019-03-21T11:58:38-07:00</updated>
  <generator build="8c85c1fbcc8c" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/pools/_new" rel="create"/>
  <link href="/services/workloads/pools/_reload" rel="_reload"/>
  <link href="/services/workloads/pools/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search_pool_1</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/pools/search_pool_1</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_1" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_1" rel="list"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_1/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_1" rel="edit"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_1" rel="remove"/>
```

```
<link href="/servicesNS/nobody/search/workloads/pools/search_pool_1/move" rel="move"/>
<link href="/servicesNS/nobody/search/workloads/pools/search_pool_1/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:key name="category">search</s:key>
    <s:key name="cpu_allocated_percent">28.57</s:key>
    <s:key name="cpu_shares">512</s:key>
    <s:key name="cpu_weight">20</s:key>
    <s:key name="default_category_pool">1</s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app">search</s:key>
        <s:key name="can_change_perms">1</s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_share_app">1</s:key>
        <s:key name="can_share_global">1</s:key>
        <s:key name="can_share_user">0</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">1</s:key>
        <s:key name="owner">nobody</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">1</s:key>
        <s:key name="sharing">app</s:key>
      </s:dict>
    </s:key>
    <s:key name="eai:attributes">
      <s:dict>
        <s:key name="optionalFields">
          <s:list>
            <s:item>cpu_weight</s:item>
            <s:item>default_category_pool</s:item>
            <s:item>default_pool</s:item>
            <s:item>ingest_pool</s:item>
            <s:item>mem_weight</s:item>
          </s:list>
        </s:key>
        <s:key name="requiredFields">
          <s:list/>
        </s:key>
        <s:key name="wildcardFields">
          <s:list/>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="mem_allocated_percent">12.00</s:key>
    <s:key name="mem_limit">12884901888</s:key>
    <s:key name="mem_weight">20</s:key>
  </s:dict>
</content>
```

```
  </entry>
</feed>
```

POST

Create and configure workload pools.

Request parameters

Name	Type	Description
cpu_weight	Number	Specifies the fraction of the cpu assigned to this pool as a ratio of the total of cpu_weight across all pools. This fraction is then applied to the cpu shares assigned to the parent group.
mem_weight	Number	You must set this value to 100 to avoid OOM errors.
category	string	Specifies the category in which a poll is created. Can be either "search", "ingest", or "misc".
default_category_pool	Boolean	Specifies the workload pool marked as default pool for its category. This property is defined per workload_pool stanza. Default is 0.
default_pool	Boolean	Specifies a workload pool defined in the search category as the default pool for the search category. **Note:** deprecated parameter retained for backwards compatibility with 7.2.x
ingest_pool	Boolean	Specifies a workload-pool defined in the ingest category as the default pool for the ingest category. **Note:** deprecated parameter retained for backwards compatibility with 7.2.x

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/pools -d name=search_pool_3 -d
category=search -d cpu_weight=40 -d mem_weight=100 -d default_category_pool=1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-pools</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/pools</id>
  <updated>2019-03-21T12:05:12-07:00</updated>
  <generator build="8c85c1fbcc8c" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/pools/_new" rel="create"/>
  <link href="/services/workloads/pools/_reload" rel="_reload"/>
  <link href="/services/workloads/pools/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search_pool_3</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/pools/search_pool_3</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3" rel="list"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3" rel="edit"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3" rel="remove"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3/move" rel="move"/>
    <link href="/servicesNS/nobody/search/workloads/pools/search_pool_3/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="category">search</s:key>
        <s:key name="cpu_allocated_percent">28.57</s:key>
        <s:key name="cpu_shares">0</s:key>
        <s:key name="cpu_weight">40</s:key>
        <s:key name="default_category_pool">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="mem_allocated_percent">36.00</s:key>
        <s:key name="mem_limit">0</s:key>
        <s:key name="mem_weight">60</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

workloads/rules

`https://<host>:<mPort>/services/workloads/rules`

Perform CRUD operations on workload rules and admission rules.

Authentication and Authorization

- GET requires the `list_workload_rules` capability.
- POST and DELETE require the `edit_workload_rules` capability.

GET

List information about workload rules and admission rules.

Request parameters

Name	Type	Description
workload_rule_type	String	Specifies the rule type. Supported values are: `search_filter`: returns admission rules only. `all`: returns both admission rules and workload rules. **Note:** To list workload rule information only, specify the endpoint URI with optional rule_name, for example services/workloads/rules/rule_name.

Returned values

Name	Type	Description
predicate	String	Specifies the predicate (condition) that a search must meet for the specified action to be taken.
action	String	Specifies the action taken when a search meets the predicate (condition).
workload_pool	String	Specifies the workload pool associated with the workload rule.
order	Boolean	Specifies the evaluation order for this workload rule amongst a group of workload rules.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/rules
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-rules</title>
  <id>https://localhost:8089/services/workloads/rules</id>
  <updated>2018-08-29T13:18:21-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/rules/_new" rel="create"/>
  <link href="/services/workloads/rules/_reload" rel="_reload"/>
```

```
<link href="/services/workloads/rules/_acl" rel="_acl"/>
<opensearch:totalResults>3</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>rule_1</title>
  <id>https://localhost:8089/servicesNS/nobody/search/workloads/rules/rule_1</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1" rel="list"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1" rel="edit"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1" rel="remove"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1/move" rel="move"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_1/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="order">3</s:key>
      <s:key name="predicate">app=search</s:key>
      <s:key name="workload_pool">default_search_pool</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>rule_2</title>
  <id>https://localhost:8089/servicesNS/nobody/search/workloads/rules/rule_2</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2" rel="alternate"/>
  <author>
```

```
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2" rel="list"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2" rel="edit"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2" rel="remove"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2/move" rel="move"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_2/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="order">1</s:key>
      <s:key name="predicate">role=admin</s:key>
      <s:key name="workload_pool">pool_1</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>rule_3</title>
  <id>https://localhost:8089/servicesNS/nobody/search/workloads/rules/rule_3</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3" rel="list"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3" rel="edit"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3" rel="remove"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3/move" rel="move"/>
  <link href="/servicesNS/nobody/search/workloads/rules/rule_3/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
```

```
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="order">2</s:key>
        <s:key name="predicate">role=analyst</s:key>
        <s:key name="workload_pool">pool_2</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Create and configure, or enable/disable a workload rule or an admission rule.

Request parameters

Name	Type	Description
name	String	Specifies the name of the workload rule or admission rule.
predicate	String	Specifies a predicate (condition) that must be true for a search to gain access to the workload pool. The syntax is <type>=<value>, with optional AND, OR, NOT, (). For example, `app=search AND role=power` maps all searches belonging to both the Search app and the power role to the designated workload pool. Valid predicate <type> are `app`, `role`, `index`, `user`, `search_type`, `search_mode`, `search_time_range`, and `runtime`. For valid predicate type values, see Predicate type values in the *Workload Management* manual. You can only specify one predicate for each workload rule. Multiple predicates are not supported.

Name	Type	Description
action	String	For workload rules: Specifies the action taken when a search meets the specified predicate (condition). Supported actions are `alert`, `move` and `abort`. For admission rules: You must specify `filter` as the action.
workload_pool	String	Specifies the workload pool associated with the workload rule. Specifies the destination workload pool for the `move` action.
order	Number	Specifies the evaluation order for this workload rule amongst a group of workload rules. For newly created rules, the order cannot be specified. It can only be specified for existing rules.
workload_rule_type	String	Supported value: `search_filter`. You must specify this parameter to enable or disable an admission rule.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/rules -d name=ruleTest2 -d
predicate="(role=user AND runtime>5m)" -d action=abort
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-rules</title>
  <id>https://localhost:8089/services/workloads/rules</id>
  <updated>2018-08-29T13:29:09-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/rules/_new" rel="create"/>
  <link href="/services/workloads/rules/_reload" rel="_reload"/>
  <link href="/services/workloads/rules/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
<entry>
    <title>ruleTest2</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/rules/ruleTest2</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2" rel="list"/>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2" rel="edit"/>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2" rel="remove"/>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2/move" rel="move"/>
    <link href="/servicesNS/nobody/search/workloads/rules/ruleTest2/disable" rel="disable"/>
    <content type="text/xml">
```

```
      <s:dict>
        <s:key name="action">abort</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="order">4</s:key>
        <s:key name="predicate">(role=user AND runtime>5m)</s:key>
        <s:key name="workload_pool"></s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

DELETE

Delete workload rules and admission rules.

Request parameters

Name	Type	Description
workload_rule_type	String	Specifies the rule to delete is an admission rule. Supported value: `search_filter`.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass -X DELETE https://localhost:8089/services/workloads/rules/rule_name
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-rules</title>
  <id>https://localhost:8089/services/workloads/rules</id>
  <updated>2018-08-29T13:29:47-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/rules/_new" rel="create"/>
  <link href="/services/workloads/rules/_reload" rel="_reload"/>
  <link href="/services/workloads/rules/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

workloads/config/enable

`https://<host>:<mPort>/services/workloads/config/enable`

Enable workload management.

Authentication and Authorization

Requires the `edit_workload_pools` capability.

POST

Enable workload management

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/config/enable
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-config</title>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-08-29T13:32:26-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <link href="/services/workloads/config/disable" rel="disable"/>
  <link href="/services/workloads/config/enable" rel="enable"/>
  <link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
  <link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

workloads/config/disable

`https://<host>:<mPort>/services/workloads/config/disable`
Endpoint to disable workload management.

Authentication and Authorization

Requires the `edit_workload_pools` capability.

POST

Disable workload management

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/config/disable
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
```

```
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-config</title>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-08-29T13:33:55-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <link href="/services/workloads/config/disable" rel="disable"/>
  <link href="/services/workloads/config/enable" rel="enable"/>
  <link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
  <link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

workloads/config/get-base-dirname

```
https://<host>:<mPort>/services/workloads/config/get-base-dirname
```

Get the name of the splunk parent cgroup.

Authentication and Authorization

Requires the `edit_workload_pools` capability.

GET

Get the name of the splunk parent cgroup.

Request parameters

None

Returned values

Name	Type	Description
workload_pool_base_dir_name	String	Specifies the parent level cgroup for splunk. **Note:** This setting applies only to systems running non-systemd setups. With systemd, this setting is ignored.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/config/get-base-dirname
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
```

```
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-config</title>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-08-29T14:49:48-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <link href="/services/workloads/config/disable" rel="disable"/>
  <link href="/services/workloads/config/enable" rel="enable"/>
  <link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
  <link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>workload-pool-base-path</title>
    <id>https://localhost:8089/services/workloads/config/workload-pool-base-path</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/workloads/config/workload-pool-base-path" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/workloads/config/workload-pool-base-path" rel="list"/>
    <link href="/services/workloads/config/workload-pool-base-path/_reload" rel="_reload"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>analyst</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="workload_pool_base_dir_name">splunk</s:key>
      </s:dict>
    </content>
  </entry>
```

```
</feed>
```

workloads/config/preflight-checks

```
https://<host>:<mPort>/services/workloads/config/preflight-checks
```

Run Linux preflight checks for workload management.

Authentication and Authorization

Requires the `list_workload_pools` and `edit_workload_pools` capabilities.

GET

Run Linux preflight checks for workload management.

Request parameters

None

Returned values

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/config/preflight-checks
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-config</title>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-11-30T14:38:15-08:00</updated>
  <generator build="611919ba3f87bb18f54b0df1b03fd86a273309c2" version="20181121"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <link href="/services/workloads/config/disable" rel="disable"/>
  <link href="/services/workloads/config/enable" rel="enable"/>
  <link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
  <link href="/services/workloads/config/preflight-checks" rel="preflight-checks"/>
  <link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>workload-management-preflight-checks</title>
    <id>https://qa-centos7x64-132:8089/services/workloads/config/workload-management-preflight-checks</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/workloads/config/workload-management-preflight-checks" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/workloads/config/workload-management-preflight-checks" rel="list"/>
    <link href="/services/workloads/config/workload-management-preflight-checks/_reload" rel="_reload"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="cgroup_version">
          <s:dict>
            <s:key name="mitigation">Cgroup version must be version 1.</s:key>
            <s:key name="preflight_check_status">1</s:key>
            <s:key name="title">Cgroup Version</s:key>
          </s:dict>
        </s:key>
        <s:key name="cpu_splunk_base_dir_permission">
          <s:dict>
            <s:key name="mitigation">CPU Splunk base directory Splunkd.service requires read and write
permissions.</s:key>
            <s:key name="preflight_check_status">1</s:key>
            <s:key name="title">CPU Splunk base directory permissions</s:key>
          </s:dict>
        </s:key>
        <s:key name="cpu_splunk_base_dir_present">
          <s:dict>
            <s:key name="mitigation">CPU Splunk base directory Splunkd.service is missing.</s:key>
            <s:key name="preflight_check_status">1</s:key>
            <s:key name="title">CPU Splunk base directory present</s:key>
          </s:dict>
        </s:key>
        <s:key name="delegate_set">
          <s:dict>
            <s:key name="mitigation">The 'Delegate' property in the unit file must be set to 'true'. Restart
Splunk then rerun preflight checks.</s:key>
            <s:key name="preflight_check_status">1</s:key>
            <s:key name="title">Delegate property set to true</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="general">
        <s:dict>
          <s:key name="preflight_checks_status">1</s:key>
          <s:key name="systemd_present">1</s:key>
        </s:dict>
      </s:key>
      <s:key name="launched_under_systemd">
        <s:dict>
          <s:key name="mitigation">In the unit file, the 'Restart' property must be set to 'always'. The
'ExecStart' property must include '_internal_launch_under_systemd'. Make sure the up-to-date unit file is
loaded.</s:key>
          <s:key name="preflight_check_status">1</s:key>
          <s:key name="title">Splunk launched under systemd</s:key>
        </s:dict>
      </s:key>
      <s:key name="memory_splunk_base_dir_permission">
        <s:dict>
          <s:key name="mitigation">Memory Splunk base directory Splunkd.service requires read and write
permissions.</s:key>
          <s:key name="preflight_check_status">1</s:key>
          <s:key name="title">Memory Splunk base directory permissions</s:key>
        </s:dict>
      </s:key>
      <s:key name="memory_splunk_base_dir_present">
        <s:dict>
          <s:key name="mitigation">Memory Splunk base directory Splunkd.service is missing.</s:key>
          <s:key name="preflight_check_status">1</s:key>
          <s:key name="title">Memory Splunk base directory present</s:key>
        </s:dict>
      </s:key>
      <s:key name="platform_type">
        <s:dict>
          <s:key name="mitigation">Operating system must be Linux.</s:key>
          <s:key name="preflight_check_status">1</s:key>
          <s:key name="title">Operating System</s:key>
        </s:dict>
      </s:key>
      <s:key name="unit_file_present">
        <s:dict>
          <s:key name="mitigation">Unit file Splunkd.service is missing. Restart Splunk then rerun
preflight checks.</s:key>
          <s:key name="preflight_check_status">1</s:key>
          <s:key name="title">Unit file present</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
 </entry>
</feed>
```

workloads/config/set-base-dirname

`https://<host>:<mPort>/services/workloads/config/set-base-dirname`

Set the name of the splunk parent cgroup.

Authentication and Authorization

Requires the `edit_workload_pools` capability.

POST

Set the name of the splunk parent cgroup.

Request parameters

Name	Type	Description
workload_pool_base_dir_name	String	Specifies the parent level cgroup for splunk. **Note:** This setting applies only to systems running non-systemd setups. With systemd, this setting is ignored.

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/config/set-base-dirname -d
"workload_pool_base_dir_name=splunkbase"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-config</title>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-08-29T14:54:31-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <link href="/services/workloads/config/disable" rel="disable"/>
  <link href="/services/workloads/config/enable" rel="enable"/>
  <link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
  <link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

workloads/policy/search_admission_control

`https://<host>:<mPort>/services/search/workloads/policy/search_admission_control`

Enable or disable admission rules.

Authentication and Authorization

- GET requires the `list_workload_policy` capability.
- POST requires the `edit_workload_policy` capability.

GET

List the enabled status of admission rules.

Request parameters

None

Returned values

Name	Type	Description
admission_rules_enabled	Boolean	Specifies the enabled status of admission rules. 0 (disabled) or 1 (enabled).

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/policy/search_admission_control
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-policy</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/policy</id>
  <updated>2020-10-10T16:55:22-07:00</updated>
  <generator build="4cd34d9fdb3b" version="8.1.2008"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/policy/_reload" rel="_reload"/>
  <link href="/services/workloads/policy/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search_admission_control</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/policy/search_admission_control</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control" rel="list"/>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control" rel="edit"/>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="admission_rules_enabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>admission_rules_enabled</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list/>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

POST

Enable or disable admission rules.

Request parameters

Name	Type	Description
admission_rules_enabled	Boolean	Enable or disable admission rules. 0 (disabled) or 1 (enabled).

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/policy/search_admission_control -d
admission_rules_enabled=1"
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-policy</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/policy</id>
  <updated>2020-10-10T17:00:58-07:00</updated>
  <generator build="4cd34d9fdb3b" version="8.1.2008"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/policy/_reload" rel="_reload"/>
  <link href="/services/workloads/policy/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search_admission_control</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/policy/search_admission_control</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control" rel="list"/>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control" rel="edit"/>
    <link href="/servicesNS/nobody/search/workloads/policy/search_admission_control/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="admission_rules_enabled">1</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

workloads/status

`https://<host>:<mPort>/services/workloads/status`
Get information on the current status of workload management.

Authentication and Authorization

Requires the `list_workload_pools` capability.

GET

Get information on the current status of workload management.

Request parameters

Name	Type	Description
advanced	Boolean	`advanced=1` returns dispatch time for each process running in each search pool.

Returned values

General information:

Name	Type	Description
default_pool	String	Specifies the workload pool marked as the default pool.
ingest_pool	Number	Specifies the workload pool marked as the ingest pool.
error_message	String	Displays the last error message observed while trying to enable workload management. This message is reset to empty on each successful enablement of workload management.
enabled	Boolean	Specifies whether or not workload management is enabled.
isSupported	Boolean	Specifies whether or not workload management is supported on this machine.
os_build	String	Specifies the operating system build information.
os_extended_name	String	Specifies the extended name of the underlying operating system.
os_name	String	Specifies the name of the underlying operating system.
os_version	String	Specifies the operating system version.

Workload pools:

Name	Type	Description
cpu_weight'	Number	Specifies the fraction of the cpu assigned to this pool as a ratio of the total of cpu_weight across all pools. This fraction is then applied to the cpu shares assigned to the parent group.
mem_weight	Number	Specifies the fraction of the memory assigned to this pool as a ratio of the total of mem_weight across all pools. This fraction is then applied to the memory limits assigned to the parent group.

Workload rules:

Name	Type	Description
predicate	String	Specifies the predicate condition that must match to access a workload pool. This must be of the format "app=<value>" or "role=<value". For example, app=itsi, role=admin. No other predicate formats are supported.
workload_pool	String	Specifies the workload pool to associate with the workload rule.
order	Number	Specifies the evaluation order for this workload rule amongst a group of workload rules.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/status
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-status</title>
  <id>https://localhost:8089/services/workloads/status</id>
  <updated>2018-08-29T13:53:48-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/status/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>workload-management-status</title>
    <id>https://localhost:8089/services/workloads/status/workload-management-status</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/workloads/status/workload-management-status" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/workloads/status/workload-management-status" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>analyst</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list/>
                </s:key>
              </s:dict>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="general">
          <s:dict>
            <s:key name="default_pool">default_search_pool</s:key>
            <s:key name="enabled">1</s:key>
            <s:key name="error_message"></s:key>
            <s:key name="ingest_pool">default_ingest_pool</s:key>
            <s:key name="isSupported">1</s:key>
            <s:key name="os_build">#1 SMP Wed Oct 19 11:24:13 EDT 2016</s:key>
            <s:key name="os_extended_name">Linux</s:key>
            <s:key name="os_name">Linux</s:key>
            <s:key name="os_version">3.10.0-514.el7.x86_64</s:key>
          </s:dict>
        </s:key>
        <s:key name="workload-pools">
          <s:dict>
            <s:key name="default_ingest_pool">
              <s:dict>
                <s:key
name="cpu_group">/sys/fs/cgroup/cpu/system.slice/Splunkd.service/default_ingest_pool</s:key>
                <s:key name="cpu_weight">25</s:key>
                <s:key
name="mem_group">/sys/fs/cgroup/memory/system.slice/Splunkd.service/default_ingest_pool</s:key>
                <s:key name="mem_weight">25</s:key>
              </s:dict>
            </s:key>
            <s:key name="default_search_pool">
              <s:dict>
                <s:key
name="cpu_group">/sys/fs/cgroup/cpu/system.slice/Splunkd.service/default_search_pool</s:key>
                <s:key name="cpu_weight">25</s:key>
                <s:key
name="mem_group">/sys/fs/cgroup/memory/system.slice/Splunkd.service/default_search_pool</s:key>
                <s:key name="mem_weight">25</s:key>
              </s:dict>
            </s:key>
            <s:key name="pool_2">
              <s:dict>
                <s:key name="cpu_group">/sys/fs/cgroup/cpu/system.slice/Splunkd.service/pool_2</s:key>
                <s:key name="cpu_weight">20</s:key>
                <s:key name="mem_group">/sys/fs/cgroup/memory/system.slice/Splunkd.service/pool_2</s:key>
                <s:key name="mem_weight">20</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="workload-rules">
          <s:dict>
            <s:key name="rule_3">
              <s:dict>
                <s:key name="order">1</s:key>
                <s:key name="predicate">role=analyst</s:key>
                <s:key name="workload_pool">pool_2</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```