



# **Splunk® Enterprise**

## **REST API Reference Manual 8.2.1**

Generated: 7/12/2021 8:28 pm

# Table of Contents

<b>Introduction.....</b>	<b>1</b>
Using the REST API reference.....	1
Endpoints reference list.....	5
<b>Access endpoints.....</b>	<b>24</b>
Access endpoint descriptions.....	24
<b>Application endpoints.....</b>	<b>192</b>
Application endpoint descriptions.....	192
<b>Cluster endpoints.....</b>	<b>218</b>
Cluster endpoint descriptions.....	218
<b>Configuration endpoints.....</b>	<b>353</b>
Configuration endpoint descriptions.....	353
<b>Deployment endpoints.....</b>	<b>370</b>
Deployment endpoint descriptions.....	370
<b>Federated Search endpoints.....</b>	<b>429</b>
Federated search endpoint descriptions.....	429
<b>Input endpoints.....</b>	<b>452</b>
Input endpoint descriptions.....	452
<b>Introspection endpoints.....</b>	<b>591</b>
Introspection endpoint descriptions.....	591
<b>Knowledge endpoints.....</b>	<b>723</b>
Knowledge endpoint descriptions.....	723
<b>KV store endpoints.....</b>	<b>862</b>
KV store endpoint descriptions.....	862
<b>License endpoints.....</b>	<b>888</b>
License endpoint descriptions.....	888
<b>Metrics Catalog endpoints.....</b>	<b>924</b>
Metrics Catalog endpoint descriptions.....	924
<b>Output endpoints.....</b>	<b>941</b>
Output endpoint descriptions.....	941
<b>Search endpoints.....</b>	<b>972</b>
Search endpoint descriptions.....	972

# Table of Contents

<b>System endpoints.....</b>	<b>1150</b>
System endpoint descriptions.....	1150
<b>Workload management endpoints.....</b>	<b>1173</b>
Workload management endpoint descriptions.....	1173

# 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.

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

### ***Splunk Cloud REST API usage***

There are some REST API access and usage differences between Splunk Cloud and Splunk Enterprise. If you are using Splunk Cloud, review details in Access requirements and limitations for the Splunk Cloud 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.
Applications	Install applications and application templates.
Clusters	Configure and manage indexer clusters and search head clusters.
Configuration	Manage configuration files and settings.
Deployment	Manage deployment servers and clients.
Inputs	Manage data input.
Introspection	Access system properties.
Knowledge	Define indexed and searched data configurations.
KV store	Manage app key-value store.
Licensing	Manage licensing configurations.
Outputs	Manage forwarder data configuration.
Search	Manage searches and search-generated alerts and view objects.
System	Manage server configuration.
Workload management	Manage system resources for search workloads.

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
<i>count</i>	Number	30	Maximum number of entries to return. Set value to 0 to get all available entries.
<i>f</i>	String		Filters the response to include only the named values. Specify multiple times to return multiple values.  Examples:  <code>f=qualifiedSearch</code> returns only the value for <code>qualifiedSearch</code> . <code>f=s*</code> returns all the values that have names beginning with <code>s</code> . <code>f=qualifiedSearch&amp;f=is_visible</code> returns the values for <code>qualifiedSearch</code> as well as <code>is_visible</code> .
<i>offset</i>	Number	0	Index of first item to return.
<i>search</i>	String		Response filter, where the response field values are matched against this search expression.  Example:  <code>search=foo</code> matches on any field with the string <code>foo</code> in the name. <code>search=field_name%3Dfield_value</code> restricts the match to a single field. (Requires URI-encoding.)
<i>sort_dir</i>	Enum	asc	Response sort order:

Name	Datatype	Default	Description
			<code>asc</code> = ascending <code>desc</code> = descending
<code>sort_key</code>	String	name	Field name to use for sorting.
<code>sort_mode</code>	Enum	auto	Collated ordering:  <code>auto</code> = If all field values are numeric, collate numerically. Otherwise, collate alphabetically. <code>alpha</code> = Collate alphabetically, not case-sensitive. <code>alpha_case</code> = Collate alphabetically, case-sensitive. <code>num</code> = Collate numerically.
<code>summarize</code>	Bool	false	Response type:  <code>true</code> = Summarized response, omitting some index details, providing a faster response. <code>false</code> = 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
-----------	-------------

<i>app</i>	The app context for the resource. Allowed values are: <ul style="list-style-type: none"> <li>• The name of an app</li> <li>• <code>system</code></li> </ul>
<i>can_list</i>	For internal use only for the Splunk Web manager UI.
<i>can_share_*</i>	Indicates whether or not the current user can change the sharing state. The sharing state can be one of: <ul style="list-style-type: none"> <li>• <code>can_share_app</code> = App-level sharing</li> <li>• <code>can_share_global</code> = Global sharing</li> <li>• <code>can_share_user</code> = User-level sharing</li> </ul>
<i>can_write</i>	Indicates whether or not the current user can edit this item.
<i>owner</i>	The user that owns the resource.  A value of <code>nobody</code> indicates that all users have access to the resource, but that write access to the resource might be restricted.
<i>modifiable</i>	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 <code>/server/logger</code> .
<i>perms.read</i>	Properties that indicate read permissions of the resource.
<i>perms.write</i>	Properties that indicate write permissions of the resource.
<i>removable</i>	Indicates if an admin or user with sufficient permissions can remove the entity.
<i>sharing</i>	Indicates how the resource is shared. Allowed values are: <ul style="list-style-type: none"> <li>• <code>app</code> = Shared through an app.</li> <li>• <code>global</code> = Shared to all apps.</li> <li>• <code>user</code> = Private to a user.</li> </ul>

**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
<i>optionalFields</i>	Field is optional.
<i>requiredFields</i>	Field is required.
<i>wildcardFields</i>	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
<code>admin/</code>					
<code>admin/LDAP-groups</code>	Access Manage LDAP authentication.				
<code>admin/metrics-reload/_metrics</code>	Access Reload the metrics processor after updating a metrics-related configuration.				
<code>admin/ProxySSO-auth</code>	Access Manage ProxySSO mappings and configurations.				
<code>admin/replicate-SAML-certs</code>	Access Manage SAML authentication.				
<code>admin/Rsa-MFA</code>	Access Configure RSA Multifactor Authentication.				
<code>admin/Rsa-MFA-config-verify/&lt;rsa-stanza-name&gt;</code>	Access Verify RSA multifactor authentication.				
<code>admin/SAML-groups</code>	Access Convert external groups in an IdP response to internal Splunk platform roles.				
<code>admin/SAML-idp-metadata</code>	Access Access IdP SAML metadata attributes.				
<code>admin/SAML-sp-metadata</code>					



URI	Summary	GET	PUT	POST	DEL
	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.				
<b>alerts/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
alerts/alert_actions	Search Access a list of alert actions				
alerts/fired_alerts	Search Access all fired alerts				
alerts/fired_alerts/{name}	Search Access specific fired alert				
<b>apps/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				
<b>authentication/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				

URI	Summary	GET	PUT	POST	DEL
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				
authentication/users/{name}	Access control Manage specific user account				
<b>authorization/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				
<b>catalog/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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}.				

URI	Summary	GET	PUT	POST	DEL
<b>cluster/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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 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/sites	Clusters Access cluster site information				
cluster/manager/sites/{name}	Clusters Access specific cluster site information				

URI	Summary	GET	PUT	POST	DEL
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				
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				
<b>configs/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
configs/conf-{file}	Configuration Raw access to .conf files				
configs/conf-{file}/{name}	Configuration Raw access to specific .conf file				
<b>data/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				

URI	Summary	GET	PUT	POST	DEL
data/indexes-extended/{name}	Indexes Access specific index bucket level information				
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				
data/inputs/tcp/raw/{name}					

URI	Summary	GET	PUT	POST	DEL
	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/splunkcptoken	Inputs Manage receiver access using tokens.				
data/inputs/tcp/splunkcptoken/{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				

URI	Summary	GET	PUT	POST	DEL
data/lookup-table-files	Knowledge Access lookup table files				
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 <code>props.conf</code> file calculated fields				
data/props/calcfields/{name}	Knowledge Manage specific <code>props.conf</code> file calculated field				
data/props/extractions	Knowledge Access <code>props.conf</code> file search-time field extractions				
data/props/extractions/{name}	Knowledge Manage specific <code>props.conf</code> file field extraction				
data/props/fieldaliases	Knowledge Access <code>props.conf</code> file field aliases				
data/props/fieldaliases/{name}	Knowledge Manage specific <code>props.conf</code> file field alias				
data/props/lookups					

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



URI	Summary	GET	PUT	POST	DEL
datamodel/model/{name}	Knowledge Access information about a data model				
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				

URI	Summary	GET	PUT	POST	DEL
<b>directory/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
directory	Knowledge Access user-configurable entities				
directory/{name}	Knowledge Manage specific entity in directory service enumeration				
<b>indexing/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
indexing/preview	Deployment Preview events from a file before indexing				
indexing/preview/{job_id}	Inputs Access <code>props.conf</code> file settings for specific data preview job				
<b>kvstore/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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.				
<b>licenser/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				

URI	Summary	GET	PUT	POST	DEL
licenser/peers/{name}	Licensing Access specific license manager peer				
licenser/stacks	Licensing Access license stack configuration				
licenser/stacks/{name}	Licensing Access specific license stack configuration				
licenser/usage	Licensing Access current usage information.				
<b>messages/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
messages	System Manage system messages				
messages/{name}	System Manage specific system message				
<b>properties/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				
<b>receivers/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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.				
<b>saved/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>

URI	Summary	GET	PUT	POST	DEL
saved/eventtypes	Knowledge Manage saved event types				
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				
<b>scheduled/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				
<b>search/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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				

URI	Summary	GET	PUT	POST	DEL
	replication configuration				
search/distributed/bundle/replication/cycles	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 <code>search.log</code> file for specific search				
search/jobs/{search_id}/summary	Search Access <code>getFieldsAndStats</code> output of so-far-read events				
search/jobs/{search_id}/timeline	Search Access event distribution over time				
search/jobs/export	Search Stream search results				

URI	Summary	GET	PUT	POST	DEL
search/parser	Search Access search language parsing services				
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				
<b>server/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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 <code>splunkd</code> health status information.				
server/health/splunkd/details	Introspection Access <code>splunkd</code> feature health status information.				
server/health-config	Introspection Access <code>splunkd</code> health report configuration information.				
server/health-config/{alert_action}	Introspection Configure alert actions for the <code>splunkd</code> health				

URI	Summary	GET	PUT	POST	DEL
	report.				
server/health-config/{feature_name}	Introspection Edit feature and indicator settings for the <code>splunkd</code> 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 <code>splunk.secret</code> 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				

URI	Summary	GET	PUT	POST	DEL
server/status/partitions-space	Introspection Access disk utilization information				
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				
<b>services/collector</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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.				
<b>shcluster/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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 <code>splunk.secret</code> key file on all nodes of a Splunk Enterprise search head cluster				



URI	Summary	GET	PUT	POST	DEL
shcluster/captain/control/default/restart	Clusters Initiate rolling restart of SHC.				
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.				
<b>storage/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
storage/passwords	Access control Manage authentication credentials				
storage/passwords/{name}	Access control Manage specific authentication credential				
<b>storage/collections</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
storage/collections/config					

URI	Summary	GET	PUT	POST	DEL
	KV store Create or list connections.				
storage/collections/config/{collection}	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.				
<b>workloads/</b>		<b>GET</b>	<b>PUT</b>	<b>POST</b>	<b>DELETE</b>
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 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 *Splunk REST API Tutorials* 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
<i>name</i>	Configuration stanza name
<i>integrationKey</i>	Duo integration key for Splunk. Must be of size = 20.
<i>secretKey</i>	Shared secret key between Splunk and Duo.
<i>apiHostname</i>	Duo REST API endpoint used by Splunk for multifactor authentication
<i>appSecretKey</i>	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
<i>failOpen</i>	Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to <i>false</i> .
<i>timeout</i>	Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.
<i>sslVersions</i>	SSL version to use for accessing the Duo REST API. Defaults to Splunkd <i>sslVersion</i> .
<i>cipherSuite</i>	Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd <i>cipherSuite</i> .
<i>ecdhCurves</i>	ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd <i>ecdhCurves</i> .
<i>sslVerifyServerCert</i>	Boolean indicating if Duo server certificate verification is required. Defaults to <i>false</i> .
<i>sslRootCAPath</i>	Full path of the certificate to be used for certificate verification if <i>sslVerifyServerCert</i> is <i>true</i> .
<i>sslCommonNameToCheck</i>	Common name to verify if <i>sslVerifyServerCert</i> is <i>true</i> .
<i>sslAltNameToCheck</i>	Alternate name to verify if <i>sslVerifyServerCert</i> is <i>true</i> .
<i>useClientSSLCompression</i>	Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd <i>useClientSSLCompression</i> .

### 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+Xl0rAfgBgQEwe+VevD/MOOfFTIA4vwoaFnCX0V0T08ZsCsKQ=</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
<i>name</i>	String	<b>Required.</b> Configuration stanza name
<i>integrationKey</i>	See description	<b>Required.</b> Duo integration key for Splunk. Must be of size = 20.
<i>secretKey</i>	See description	<b>Required.</b> Shared secret key between Splunk and Duo.
<i>apiHostname</i>	See description	<b>Required.</b> Duo REST API endpoint used by Splunk for multifactor authentication
<i>appSecretKey</i>	See description	<b>Required.</b> Splunk application specific secret key. Must be a random generated hex of length 40 or more.
<i>failOpen</i>	Boolean	Optional. Indicates whether Splunk should bypass the Duo service if it is unavailable. Defaults to <code>false</code> .
<i>timeout</i>	Positive integer	Optional. Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.
<i>sslVersions</i>	See description	Optional. SSL version to use for accessing the Duo REST API. Defaults to Splunkd <code>sslVersion</code> .
<i>cipherSuite</i>	See description	Optional. Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd <code>cipherSuite</code> .
<i>ecdhCurves</i>	See description	Optional. ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd <code>ecdhCurves</code> .
<i>sslVerifyServerCert</i>	Boolean	Optional. Indicates if Duo server certificate verification is required. Defaults to <code>false</code> . If set to <code>true</code> , provide a <i>sslRootCAPath</i> to ensure successful certificate validation.
<i>sslRootCAPath</i>	See description	Optional. Full path of the certificate to be used for certificate verification. If <i>sslVerifyServerCert</i> is <code>true</code> , this path must be provided to ensure successful certificate validation.
<i>sslCommonNameToCheck</i>	See description	Optional. Common name to verify if <i>sslVerifyServerCert</i> is <code>true</code> .
<i>sslAltNameToCheck</i>	See description	Optional. Alternate name to verify if <i>sslVerifyServerCert</i> is <code>true</code> .
<i>useClientSSLCompression</i>	See description	Optional. Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd <code>useClientSSLCompression</code> .

### Returned values

Name	Description
<i>name</i>	Configuration stanza name
<i>integrationKey</i>	Duo integration key for Splunk. Must be of size = 20.
<i>secretKey</i>	Shared secret key between Splunk and Duo.

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

## Example request and response

### XML Request

```
curl -k -u admin:changeme -X POST https://localhost:8089/services/admin/Duo-MFA/duo-mfa -d
integrationKey=DIOXYOKGDJNK4JRRTOKT -d secretKey=DABZXYbRVW2yqvTM6fPVMkbgxBna0HTuYa9XuCQ2 -d
appSecretKey=56a15e48ec796f3d6ee2763b088f8ca77109692c -d apiHostname=api-cc7a8eab.duosecurity.com -d
failOpen=false -d timeout=10 -d sslVersions=tlsl.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
<i>name</i>	Configuration stanza name
<i>integrationKey</i>	Duo integration key for Splunk. Must be of size = 20.
<i>secretKey</i>	Shared secret key between Splunk and Duo.
<i>apiHostname</i>	Duo REST API endpoint used by Splunk for multifactor authentication
<i>appSecretKey</i>	Splunk application specific secret key. Must be a random generated hex of length 40 or more.
<i>failOpen</i>	Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to <code>false</code> .
<i>timeout</i>	Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.
<i>sslVersions</i>	SSL version to use for accessing the Duo REST API. Defaults to Splunkd <code>sslVersion</code> .
<i>cipherSuite</i>	Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd <code>cipherSuite</code> .
<i>ecdhCurves</i>	ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd <code>ecdhCurves</code> .
<i>sslVerifyServerCert</i>	Boolean indicating if Duo server certificate verification is required. Defaults to <code>false</code> .
<i>sslRootCAPath</i>	Full path of the certificate to be used for certificate verification if <i>sslVerifyServerCert</i> is <code>true</code> .
<i>sslCommonNameToCheck</i>	Common name to verify if <i>sslVerifyServerCert</i> is <code>true</code> .
<i>sslAltNameToCheck</i>	Alternate name to verify if <i>sslVerifyServerCert</i> is <code>true</code> .
<i>useClientSSLCompression</i>	Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd <code>useClientSSLCompression</code> .

### 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/MOOfFTIA4vwoaFnCX0V0T08ZsCsKQ=</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>

```

```

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

```

## POST

Update the `{name}` Duo Multifactor configuration.

### Request parameters

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

### Returned values

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

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

## 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"/>
</entry>
```

```

<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+Xl0rAfgBgQEwe+VevD/M00FFtIA4vwoaFnCX0123T08ZsCsKQ=</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
<i>name</i>	Configuration stanza name
<i>authManagerUrl</i>	URL of REST endpoint of RSA Authentication Manager.
<i>accessKey</i>	Access key needed by Splunk to communicate with RSA Authentication Manager. Note that this value is hidden output.
<i>clientId</i>	Agent name created on RSA Authentication Manager is clientId.
<i>failOpen</i>	If true, allow login in case authentication server is unavailable.
<i>timeout</i>	It determines the connection timeout in seconds for the outbound HTTPS connection.
<i>messageOnError</i>	Message that will be shown to user in case of login failure.
<i>enableMfaAuthRest</i>	If true, enable authentication of REST calls.
<i>caCertBundlePayload</i>	SSL certificate chain return by RSA server.
<i>replicateCertificates</i>	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:dict>

      </s:key>

    </s:dict>

  </content>

</entry>

```



```

    <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
------	------	-------------



hZcjswHQYDVR00BBYEFKZPYB4fLdHn8SogKpUW%0A5Oia6m5IMIGBBgNVHREEEjB4gg93d3cuZXhhbXBsZS5vcmeCC2V4YW1wbGUuY29t%0AggtleGFtcGx1LmVkdYILZXXhhbXBsZS5uZXSCC2V4YW1wbGUub3Jngg93d3cuZXhh%0AbXBsZS5jb2CD3d3dy5leGFtcGx1LmVkdYIPd3d3LmV4YW1wbGUubmV0MA4GA1Ud%0ADwEB%2FwQEAWIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwdQYDVR0f%0ABG4wbDA0oDKgMIYuaHR0cDovL2NybdMuZGlnaWN1cnQuY29tL3NoYTItaGEnc2Vy%0AdmVyLWc0LmNybdDA0oDKgMIYuaHR0cDovL2NybdQuZGlnaWN1cnQuY29tL3NoYTIt%0AaGEnc2VydMvYlWc0LmNybdBMBgNVHSAERTBDMDcGCWCGSAGG%2FWwBATAqMCgGCCsG%0AAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydcC5jb20vQ1BTMAgGBmeBDAECAjCB%0AgwYIKwYBBQUHAQEEdzB1MCQGCGCsGAQUFBzABhhodHRwOi8vb2NzcC5kaWdpY2Vy%0AdC5jb20wTQYIKwYBBQUHMAKGQWh0dHA6Ly9jYWN1cnRzLmRpZ21jZXJ0LmNvbS9E%0AaWdpQ2VydFNIQTJlIaWdoQXNzdXJhbmNlU2VydMvYlWc0LmNybdDA0oDKgMIYuaHR0cDovL2NybdQuZGlnaWN1cnQuY29tL3NoYTItaGEnc2FwQc%0AMAAwdQYJKoZIhvcNAQELBQADggEBAISomhGn2L0LJn5SJHuyVZ3qMl1RCIdvqe0Q%0A6ls%2BC8ctRwRO3UU3x8q8OH%2B2ahx1QmpzdC5al4XQzJLiLjiJ2Q1p%2Bhub8MFiMmVP%0APZjb2tZm2ipWVuMRM%2BzgpRVM6nVJ9F3vFfUSHOb4%2FJsEIUvPY%2Bd8%2FKrc%2BkPQwLvy%0AieqRbcuFjmgyfPmUv1U9QoI4TQikpw7TZU0zYZANP4C%2Fgj4Ry48%2FznmUaRvy2kvi%0Al7gRQ21qJTK5suoioYNo3J9T%2BpXPGU7Lydz%2FHwW%2Bw0DpArtAauki8aNX4ohFUKS%0AwDSiIWIWJiJGbEeIO0TIFwEVWTONbNl%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:dict>

    </s:key>

  </s:dict>

</content>

```

```

        </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 multifactor authentication.

### Request parameters

Name	Type	Description
<i>username'</i>	String	Optional. RSA username.
<i>passcode</i>	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, 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
<i>strategy</i>	LDAP strategy name
<i>LDAPgroup</i>	LDAP group name

### Returned values

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

Name	Description
<i>roles</i>	Roles mapped to this group
<i>strategy</i>	Strategy name
<i>type</i>	Group type
<i>users</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
```

```

        </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
<i>strategy</i>	<b>Required.</b> LDAP strategy name
<i>LDAPgroup</i>	<b>Required.</b> LDAP group name

### Returned values

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

### 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
<i>strategy</i>	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"/>
  </entry>
</feed>
```

```

<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=Sam1 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=Sam1 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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

<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}](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:dict>
  </content>
</entry>
```

```

    <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
<i>defaultRoleIfMissing</i>	Name of default role to use if no mapping is found.
<i>blacklistedUsers</i>	Comma separated list of blacklisted users.
<i>blacklistedAutoMappedRoles</i>	Comma separated list of blacklisted roles.



```

        </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
<i>name</i>	String	<b>Required.</b> New ProxySSO configuration name
<i>defaultRoleIfMissing</i>	Role name	Specify a default role to use if no mapping is found.
<i>blacklistedUsers</i>	Comma separated list	Specify blacklisted users.
<i>blacklistedAutoMappedRoles</i>	Comma separated list	Specify blacklisted roles.

### Returned values

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

```
        </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
<i>defaultRoleIfMissing</i>	Name of default role to use if no mapping is found.
<i>blacklistedUsers</i>	Comma separated list of blacklisted users.
<i>blacklistedAutoMappedRoles</i>	Comma separated list of blacklisted roles.
<i>disabled</i>	Boolean value indicating whether the configuration is disabled. 0 indicates that the configuration is enabled.
<i>title</i>	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
<i>name</i>	String	<b>Required.</b> New ProxySSO configuration name
<i>defaultRoleIfMissing</i>	Role name	Specify a default role to use if no mapping is found.
<i>blacklistedUsers</i>	Comma separated list	Specify blacklisted users.
<i>blacklistedAutoMappedRoles</i>	Comma separated list	Specify blacklisted roles.

### Returned values

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

### 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 <code>roles</code> 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 <code>roles</code> 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 <code>roles</code> 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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```



```

        </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, 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
<i>roles</i>	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:list>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

        <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
<i>name</i>	String	External group name.
<i>roles</i>	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
<i>idpMetadataFile</i>	File path. See description.	Full path of the metadata file location. File should be local to splunkd server.

### Response keys

Name	Description
<i>idpMetadataPayload</i>	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"/>
</entry>
```



```
<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[MIIDpjCCAo6gAwIBAgIGAUI7gBZ6oMAOGCSqGSIB3DQEBBQUAMIGTMQswCQYDVQQGEwJVUz
ETMBEG
A1UECAwKQ2FsaWZvcrterye444uIEZyYW5jaXNjbzENMASGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFDASBgNVBAMMC3NwbHVua3Rlc3QxMRwwGgYJKoZIhvcNAQkB
FglpbmZvQG9rdGEuY29tMB4XDTE1MDczMDE3MzEyMVVoXDTQ1MDczMDE3MzIyMVowGZMxCzAJBgNV
BAYTAInJhbmNpc2NvMQ0wCwYD
VQQKDARPa3RhMRQwEgYDVQQQLDAtTU09Qcm92aWRlcjEUMBIGA1UEAwwLc3BsdW5rdGVzdDExHDAa
BgkqhkiG9w0BCQEWDLwLm9Ab2t0YS5jb20wggeiMAOGCSqGSIB3DQEBQUAA4IBDwAwggEKAoIB
AQCS0Zh/PCBRsbHkJhi6RtGSKezFjPZyPyFr2ND9KysDf4WRgMiklOBdrlM/+BjKqPCTYFbt/L
ZXnVqo7v9wJ538MrTp6oliBi52zhpDnqAoOIrlSaB0PbbQVd/oz49YbEW6/ThsAMHdIyz3/CSqEM
o6oD7GiQzoGH4jidhx1Gjgmfk2OdkKANWQDmZGKAMHJQXtjfrUK3y0H5j2tla9iIPLUVDyopzWNa
o8TKw68iWDZs9ZGrwu9ptF4fpjiaslkWp3oyO1FmAencabXMddFZ7HgVziI2TjbExNa+bzS9SUhY
gZlf2meD/ib2ul6HVFk1VM0IJA56qWGImlJRzGj1AgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAC+I
566v40xTmhfjTlF3sRGjbXQDnJGXcuF1GFkAp/IEmdo
7mawu7Z7qcHb2BcQiVViuhY5ON20/gbz5ggDipc803JMD7dTtFxDthfZgVn1tE/nPNgx2QAKCADw
FkhYwAf6R7zV1VvyRfUzmbbl6V9JZh7Mju0vFsVJUsGhsAqJfZwQ+QckedB/Nlpr9OxBu4IYgMZ4
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/exk4nkqgsypk32FMF0h7/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
<i>spMetadataPayload</i>	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
BlNwbHVuazEXMBUGA1UEAwOU3BsdW5rQ29tbW9uQ0ExITAfBgkqhkiG9w0BCQEW
EnN1cHBvcnRac3BsdW5rLmNvbTAeFw0xNTA3Mjg3NjMzNDNaFw0xODA3MjcxNjMz
NDNaMDcxIDAeBgNVBAMMF1NwbHVrTRer55ZlckRlZmFlbHRDZXJ0MRMwEQYDVQQK
DApTcGxlbmtVc2VyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmxUfArn3l
Pxn24lBlpWDFg5VCB/f8IS7MlEFPJiepioAli+yE7exlzd0wRniw2AkiyglKbt9
zNelz9DxilfEOailFaV5ryENabYgYJFJonZKWucNvWzde50Cn4fm1nNqVSOH90F
9zTGCD7Kkem0hIqx506TI2C2dKP+cJWeWwIDAQABMA0GCSqGSIb3DQEBAQUAA4GB
ADy75DKIEgJo2AL0Zsckvrl1qGZ2+g/xBupuRBDBSRp9vs3VqN+wB39uDtMzXlZ1
u0J50hPVMdq00RJuYzZmFpAhCX4hFfsNeazfFzSK/DQCURvfYG4pZit3P8gJ6uDv
3OxcDGUorMNLGRRO61UAkrLUyWE44MMsljgidDw2QlMY
</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>
]]]></s:key>
    </s:dict>
  </content>
</entry>

```

```
</md:SPSSODescriptor> </md:EntityDescriptor> ]]></s:key>
</s:dict>
</content>
</entry>
```

---

## admin/SAML-user-role-map

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

### Description

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
<i>name</i>	SAML username for running saved searches.
<i>roles</i>	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
<i>name</i>	String	SAML username for running saved searches.

Name	Type	Description
<i>roles</i>	String	Assigned roles for this user.

## Response keys

Name	Description
<i>name</i>	SAML username for running saved searches.
<i>roles</i>	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
<i>name</i>	SAML username for running saved searches.
<i>roles</i>	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:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

```

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

```

```

        </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
<i>allowSslCompression</i>	Indicates whether ssl data compression is enabled.
<i>assertionConsumerServiceUrl</i>	Endpoint where SAML assertions are posted by the IdP.
<i>attributeAliasMail</i>	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
<i>attributeAliasRealName</i>	Specifies which SAML attribute maps to 'realName'. Defaults to <code>realName</code> .
<i>attributeAliasRole</i>	Specifies which SAML attribute maps to <code>role</code> . Defaults to <code>role</code> .
<i>attributeQueryRequestSigned</i>	Indicates whether Attribute Queries should be signed.
<i>attributeQueryResponseSigned</i>	Indicates whether Attribute Query responses should be signed.
<i>attributeQuerySoapPassword</i>	Credentials for making Attribute Query using SOAP over HTTP.
<i>attributeQuerySoapUsername</i>	Credentials for making Attribute Query using SOAP over HTTP.
<i>attributeQueryTTL</i>	ttl (time to live) for the Attribute Query credentials cache.
<i>blacklistedAutoMappedRoles</i>	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
<i>blacklistedUsers</i>	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.

Name	Description
<i>caCertFile</i>	File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem
<i>cipherSuite</i>	Ciphersuite for making Attribute Queries using ssl. For example, TLSv1+HIGH:@STRENGTH.
<i>defaultRoleIfMissing</i>	Default role to use if no role is returned in a SAML response.
<i>ecdhCurves</i>	EC curves for ECDH/ECDHE key exchange - ssl setting.
<i>entityId</i>	Unique id preconfigured by the IdP.
<i>errorUrl</i>	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or Splunk deployment.
<i>errorUrlLabel</i>	Label or title of the content to which errorUrl points. Defaults to Click here to resolve SAML error..
<i>fqdn</i>	Load balancer url.
<i>idpAttributeQueryUrl</i>	IdP attribute query url where SAML attribute queries are sent.
<i>idpCertPath</i>	Path for IdP certificate.
<i>idpSLOUrl</i>	IdP sso url where SAML SSO requests are sent.
<i>idpSSOUrl</i>	IdP SSO url where SAML SLO requests are sent.
<i>maxAttributeQueryQueueSize</i>	Maximum number of Attribute jobs to queue.
<i>maxAttributeQueryThreads</i>	Maximum number of threads for asynchronous Attribute Queries.
<i>name</i>	Configuration stanza name.
<i>nameIdFormat</i>	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
<i>redirectAfterLogoutToUrl</i>	Redirect URL after user logout If no SLO URL is configured.
<i>redirectPort</i>	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.
<i>signAuthnRequest</i>	Indicates whether to sign authentication requests.
<i>signatureAlgorithm</i>	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: <ul style="list-style-type: none"> <li>• RSA-SHA1 (default) <ul style="list-style-type: none"> <li>♦ corresponds to http://www.w3.org/2000/09/xmldsig#rsa-sha1</li> </ul> </li> <li>• RSA-SHA256 <ul style="list-style-type: none"> <li>♦ corresponds to http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</li> </ul> </li> </ul>
<i>signedAssertion</i>	Indicates whether to sign SAML assertions.
<i>singleLogoutServiceUrl</i>	URL where the IdP posts SAML Single Logout responses.
<i>skipAttributeQueryRequestForUsers</i>	

Name	Description
	Used in conjunction with <code>defaultRoleIFMissing</code> . Indicates whether to skip Attribute Queries for some users.
<i>sloBinding</i>	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . This binding must match the binding configured on the IDP.
<i>spCertPath</i>	Service provider certificate path.
<i>sslAltNameToCheck</i>	Alternate name to check in the peer certificate.
<i>sslCommonNameToCheck</i>	Common name to check in the peer certificate.
<i>sslKeysfile</i>	Location of service provider private key.
<i>sslKeysfilePassword</i>	SSL password.
<i>sslVerifyServerCert</i>	Indicates whether to verify peer certificate.
<i>sslVersions</i>	SSL versions.
<i>ssoBinding</i>	Binding used when making a SP-initiated SAML request. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . This binding must match the binding configured on the IDP.
<i>uiStatusPage</i>	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://sol: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://sol</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:dict>
  </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://sol: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
<i>allowSslCompression</i>	Indicates whether ssl data compression is enabled.
<i>attributeAliasMail</i>	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
<i>attributeAliasRealName</i>	Specifies which SAML attribute maps to 'realName'. Defaults to <code>realName</code> .
<i>attributeAliasRole</i>	Specifies which SAML attribute maps to <code>role</code> . Defaults to <code>role</code> .
<i>attributeQueryRequestSigned</i>	Indicates whether Attribute Queries should be signed.
<i>attributeQueryResponseSigned</i>	Indicates whether Attribute Query responses should be signed.
<i>attributeQuerySoapPassword</i>	Credentials for making Attribute Query using SOAP over HTTP.
<i>attributeQuerySoapUsername</i>	Credentials for making Attribute Query using SOAP over HTTP.
<i>attributeQueryTTL</i>	ttl (time to live) for the Attribute Query credentials cache.
<i>blacklistedAutoMappedRoles</i>	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
<i>blacklistedUsers</i>	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.

Name	Description
<i>caCertFile</i>	File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem
<i>cipherSuite</i>	Ciphersuite for making Attribute Queries using ssl. For example, TLSv1+HIGH:@STRENGTH.
<i>defaultRoleIfMissing</i>	Default role to use if no role is returned in a SAML response.
<i>ecdhCurves</i>	EC curves for ECDH/ECDHE key exchange - ssl setting.
<i>entityId</i>	<b>Required.</b> Unique id preconfigured by the IdP.
<i>errorUrl</i>	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or the Splunk deployment.
<i>errorUrlLabel</i>	Label or title of the content to which errorUrl points. Defaults to Click here to resolve SAML error..
<i>fqdn</i>	Load balancer url.
<i>idpAttributeQueryUrl</i>	IdP attribute query url where SAML attribute queries are sent.
<i>idpCertPath</i>	Path for IdP certificate.
<i>idpMetadataFile</i>	Full path to idpMetadata on disk. Used to retrieve IdP information such as idpSLOUrl, idpSSOUrl, and signing certificate.
<i>idpSLOUrl</i>	IdP sso url where SAML SSO requests are sent.
<i>idpSSOUrl</i>	<b>Required.</b> IdP SSO url where SAML SLO requests are sent.
<i>name</i>	<b>Required.</b> Configuration stanza name.
<i>nameIdFormat</i>	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
<i>redirectAfterLogoutToUrl</i>	Redirect URL after user logout If no SLO URL is configured.
<i>redirectPort</i>	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.
<i>signAuthnRequest</i>	Indicates whether to sign authentication requests.
<i>signatureAlgorithm</i>	Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when <i>signedAuthnRequest</i> is set to true.  Possible values are: <ul style="list-style-type: none"><li>• RSA-SHA1 (default)     ♦ corresponds to http://www.w3.org/2000/09/xmldsig#rsa-sha1</li><li>• RSA-SHA256     ♦ corresponds to http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</li></ul>
<i>signedAssertion</i>	Indicates whether to sign SAML assertions.
<i>skipAttributeQueryRequestForUsers</i>	Used in conjunction with <i>defaultRoleIfMissing</i> . Indicates whether to skip Attribute Queries for some users.
<i>sloBinding</i>	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

Name	Description
	binding configured on the IDP.
<i>sslAltNameToCheck</i>	Alternate name to check in the peer certificate.
<i>sslCommonNameToCheck</i>	Common name to check in the peer certificate.
<i>sslKeysfile</i>	Location of service provider private key.
<i>sslKeysfilePassword</i>	SSL password.
<i>sslVerifyServerCert</i>	Indicates whether to verify peer certificate.
<i>sslVersions</i>	SSL versions.
<i>ssoBinding</i>	Binding used when making a SP-initiated SAML request. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . 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"/>
</entry>
```

```

<content type="text/xml">
  <s:dict>
    <s:key name="allowSslCompression">true</s:key>
    <s:key name="assertionConsumerServiceUrl">http://sol: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://sol</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:dict>
    </s:key>
  </s:dict>
</content>

```

```

        <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://sol: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
<i>allowSslCompression</i>	Indicates whether ssl data compression is enabled.
<i>assertionConsumerServiceUrl</i>	Endpoint where SAML assertions are posted by the IdP.
<i>attributeAliasMail</i>	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
<i>attributeAliasRealName</i>	Specifies which SAML attribute maps to 'realName'. Defaults to <code>realName</code> .

Name	Description
<i>attributeAliasRole</i>	Specifies which SAML attribute maps to <code>role</code> . Defaults to <code>role</code> .
<i>attributeQueryRequestSigned</i>	Indicates whether Attribute Queries should be signed.
<i>attributeQueryResponseSigned</i>	Indicates whether Attribute Query responses should be signed.
<i>attributeQuerySoapPassword</i>	Credentials for making Attribute Query using SOAP over HTTP.
<i>attributeQuerySoapUsername</i>	Credentials for making Attribute Query using SOAP over HTTP.
<i>attributeQueryTTL</i>	ttl (time to live) for the Attribute Query credentials cache.
<i>blacklistedAutoMappedRoles</i>	Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.
<i>blacklistedUsers</i>	Comma separated list of user names from the IDP response to be blacklisted by Splunk software.
<i>caCertFile</i>	File path for CA certificate. For example, <code>/home/user123/saml-install/etc/auth/server.pem</code>
<i>cipherSuite</i>	Ciphersuite for making Attribute Queries using ssl. For example, <code>TLsv1+HIGH:@STRENGTH</code> .
<i>defaultRoleIfMissing</i>	Default role to use if no role is returned in a SAML response.
<i>ecdhCurves</i>	EC curves for ECDH/ECDHE key exchange - ssl setting.
<i>entityId</i>	Unique id preconfigured by the IdP.
<i>errorUrl</i>	URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or Splunk deployment.
<i>errorUrlLabel</i>	Label or title of the content to which errorUrl points. Defaults to <code>Click here to resolve SAML error..</code>
<i>fqdn</i>	Load balancer url.
<i>idpAttributeQueryUrl</i>	IdP attribute query url where SAML attribute queries are sent.
<i>idpCertPath</i>	Path for IdP certificate.
<i>idpSLOUrl</i>	IdP sso url where SAML SSO requests are sent.
<i>idpSSOUrl</i>	IdP SSO url where SAML SLO requests are sent.
<i>maxAttributeQueryQueueSize</i>	Maximum number of Attribute jobs to queue.
<i>maxAttributeQueryThreads</i>	Maximum number of threads for asynchronous Attribute Queries.
<i>name</i>	Configuration stanza name.
<i>nameIdFormat</i>	Specifies how subject is identified in SAML Assertion. Defaults to <code>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</code> Override it when using Azure AD as an IDP and set it to <code>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</code>
<i>redirectAfterLogoutToUrl</i>	Redirect URL after user logout If no SLO URL is configured.
<i>redirectPort</i>	Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The <code>assertionconsumerServiceUrl</code> in the <code>AuthNRequest</code> uses the set port instead of the <code>splunkweb</code> port. To prevent any port information being appended to the <code>assertionConsumerServiceUrl</code> , set to 0.
<i>signAuthnRequest</i>	Indicates whether to sign authentication requests.

Name	Description
<i>signatureAlgorithm</i>	<p>Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when <i>signedAuthnRequest</i> is set to <code>true</code>.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• RSA-SHA1 (default) <ul style="list-style-type: none"> <li>♦ corresponds to <code>http://www.w3.org/2000/09/xmldsig#rsa-sha1</code></li> </ul> </li> <li>• RSA-SHA256 <ul style="list-style-type: none"> <li>♦ corresponds to <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</code></li> </ul> </li> </ul>
<i>signedAssertion</i>	Indicates whether to sign SAML assertions.
<i>singleLogoutServiceUrl</i>	URL where the IdP posts SAML Single Logout responses.
<i>skipAttributeQueryRequestForUsers</i>	Used in conjunction with <code>defaultRoleIFMissing</code> . Indicates whether to skip Attribute Queries for some users.
<i>sloBinding</i>	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . This binding must match the binding configured on the IDP.
<i>spCertPath</i>	Service provider certificate path.
<i>sslAltNameToCheck</i>	Alternate name to check in the peer certificate.
<i>sslCommonNameToCheck</i>	Common name to check in the peer certificate.
<i>sslKeysfile</i>	Location of service provider private key.
<i>sslKeysfilePassword</i>	SSL password.
<i>sslVerifyServerCert</i>	Indicates whether to verify peer certificate.
<i>sslVersions</i>	SSL versions.
<i>ssoBinding</i>	Binding used when making a SP-initiated SAML request. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . This binding must match the binding configured on the IDP.
<i>uiStatusPage</i>	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://sol: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://sol</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://sol: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
<i>allowSslCompression</i>	Indicates whether ssl data compression is enabled.
<i>attributeAliasMail</i>	Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.
<i>attributeAliasRealName</i>	Specifies which SAML attribute maps to 'realName'. Defaults to <code>realName</code> .
<i>attributeAliasRole</i>	Specifies which SAML attribute maps to <code>role</code> . Defaults to <code>role</code> .

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

Name	Description
	<ul style="list-style-type: none"> <li>• RSA-SHA1 (default) <ul style="list-style-type: none"> <li>♦ corresponds to <a href="http://www.w3.org/2000/09/xmldsig#rsa-sha1">http://www.w3.org/2000/09/xmldsig#rsa-sha1</a></li> </ul> </li> <li>• RSA-SHA256 <ul style="list-style-type: none"> <li>♦ corresponds to <a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</a></li> </ul> </li> </ul>
<i>signedAssertion</i>	Indicates whether to sign SAML assertions.
<i>skipAttributeQueryRequestForUsers</i>	Used in conjunction with <code>defaultRoleIFMissing</code> . Indicates whether to skip Attribute Queries for some users.
<i>sloBinding</i>	Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . This binding must match the binding configured on the IDP.
<i>sslAltNameToCheck</i>	Alternate name to check in the peer certificate.
<i>sslCommonNameToCheck</i>	Common name to check in the peer certificate.
<i>sslKeysfile</i>	Location of service provider private key.
<i>sslKeysfilePassword</i>	SSL password.
<i>sslVerifyServerCert</i>	Indicates whether to verify peer certificate.
<i>sslVersions</i>	SSL versions.
<i>ssoBinding</i>	Binding used when making a SP-initiated SAML request. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code> . 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://sol12800/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://sol1</s:key>
    <s:key name="idpCertChains">
      <s:list/>
    </s:key>
    <s:key name="idpCertPath"></s:key>
    <s:key name="maxAttributeQueryQueueSize">100</s:key>
  </s:dict>
</content>

```

```

<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://sol: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/disable

```

---

## authentication/providers/SAML/{stanza\_name}/disable

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

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

### Response data keys

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

Name	Description
<i>sessionKey</i>	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>8Q1QczpArNgKqfUmkmhwiZVer4^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
<i>capabilities</i>	List of capabilities assigned to role.

Name	Description
<i>defaultApp</i>	Default app for the user, which is invoked at login.
<i>defaultAppIsUserOverride</i>	Default app override indicates: true = Default app overrides the user role default app. false = Default app does not override the user role default app.
<i>defaultAppSourceRole</i>	The role that determines the default app for the user, if the user has multiple roles.
<i>email</i>	User email address.
<i>password</i>	User password.
<i>realname</i>	User full name.
<i>restart_background_jobs</i>	Restart background search job that has not completed when Splunk restarts indication: true = Restart job. false = Do not restart job.
<i>roles</i>	Roles assigned to the user.
<i>type</i>	User authentication system type: <ul style="list-style-type: none"> <li>• LDAP</li> <li>• Scripted</li> <li>• Splunk</li> <li>• System (reserved for system user)</li> </ul>
<i>tz</i>	User timezone.
<i>username</i>	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_wmicconf</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:list>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

    <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
<i>authString</i>	Unique identifier for this session.
<i>searchId</i>	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.
<i>timeAccessed</i>	Last time the session was touched.
<i>userName</i>	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">1RU5vGFm2OPq29p1LtvtqlEB9xzPDLZ3AleUhElbwPjIrKtvyLE4fODhs^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">1RU5vGFm2OPq29p1LtvqlEB9xzPDLZ3AleUhE1bwPjIrKtvyle4fODhs^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:dict>
        </s:key>
      </s:dict>
    </s:key>
  </content>
</entry>
</s:messages>
</s:messages>
```



```

        <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
<i>authString</i>	Unique session identifier.
<i>searchId</i>	Session search ID, if it is a search job session. The value is blank for a login-type session.
<i>timeAccessed</i>	Last time the session was touched.
<i>userName</i>	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
<i>capabilities</i>	List of capabilities assigned to role.
<i>defaultApp</i>	Default app for the user, which is invoked at login.
<i>defaultAppIsUserOverride</i>	Default app override indicates: <code>true</code> = Default app overrides the user role default app. <code>false</code> = Default app does not override the user role default app.
<i>defaultAppSourceRole</i>	The role that determines the default app for the user, if the user has multiple roles.
<i>email</i>	User email address.
<i>password</i>	User password.
<i>realname</i>	User full name.
<i>restart_background_jobs</i>	Restart background search job that has not completed when Splunk restarts indication: <code>true</code> = Restart job. <code>false</code> = Do not restart job.
<i>roles</i>	Roles assigned to the user.
<i>type</i>	One of the following user authentication system types. <ul style="list-style-type: none"><li>• <code>LDAP</code></li><li>• <code>Scripted</code></li><li>• <code>Splunk</code></li><li>• <code>System</code> (reserved for system user)</li></ul>
<i>tz</i>	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
<i>createrole</i>	Boolean	<p>Flag to indicate that a new role should be created for the user. If set to "true", the new role <code>user-&lt;name&gt;</code> is created and assigned to the user. The <code>&lt;name&gt;</code> portion of the new role matches the <code>name</code> parameter value passed in with this POST request.</p> <p>If set to "false", at least one existing role must be specified using the <code>roles</code> parameter for the POST request.</p> <p>Defaults to "false".</p>
<i>defaultApp</i>	String	User default app. Overrides the default app inherited from the user roles.
<i>email</i>	String	User email address.
<i>force-change-pass</i>	Boolean	<p>Force user to change password indication:</p> <p><code>true</code> = Force password change.</p> <p><code>false</code> = Do not force password change.</p>
<i>name</i>	String	<b>Required.</b> Unique user login name.
<i>password</i>	String	User login password.
<i>realname</i>	String	Full user name.
<i>restart_background_jobs</i>	Boolean	<p>Restart background search job that has not completed when Splunk restarts indication:</p> <p><code>true</code> = Restart job.</p> <p><code>false</code> = Do not restart job.</p>
<i>roles</i>	String	<p>Role to assign to this user. To assign multiple roles, pass in each role using a separate <code>roles</code> parameter value.</p> <p>For example, <code>-d roles="role1", -d roles="role2"</code>.</p> <p>At least one existing role is required if you are not using the <code>createrole</code> parameter to create a new role for the user. If you are using <code>createrole</code> to create a new role, you can optionally use this parameter to specify additional roles to assign to the user.</p>
<i>tz</i>	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:list>
      </s:key>
    </s:dict>
  </content>
</entry>
```

```

    <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_wmicnf</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: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 capabilities, 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_wmicnf</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:list>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

    <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
<i>capabilities</i>	List of capabilities assigned to role.
<i>defaultApp</i>	Default app for the user, which is invoked at login.
<i>defaultApplsUserOverride</i>	Default app override indicator. true = Default app overrides the user role default app. false = Default app does not override the user role default app.
<i>defaultAppSourceRole</i>	Role that determines the default app for the user, if the user has multiple roles.
<i>email</i>	User email address
<i>password</i>	User password
<i>realname</i>	User full name
<i>restart_background_jobs</i>	Indicates whether incomplete background search jobs restart when the Splunk deployment restarts. true = Restart jobs. false = Do not restart jobs.
<i>roles</i>	Roles assigned to the user.
<i>type</i>	One of the following user authentication system types. <ul style="list-style-type: none"> <li>• LDAP</li> <li>• Scripted</li> <li>• Splunk</li> <li>• System (reserved for system user)</li> </ul>
<i>tz</i>	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:list>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

    <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
<i>defaultApp</i>	String	User default app. This overrides the default app inherited from the user roles.
<i>email</i>	String	User email address.
<i>force-change-pass</i>	Boolean	Indicates whether to force user password change. <i>true</i> = Force password change. <i>false</i> = Do not force password change.
<i>oldpassword</i>	String	Old user login password. Only <b>required</b> if using the <i>password</i> parameter to change the current user's password.
<i>password</i>	String	<b>Required.</b> 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 <i>oldpassword</i> parameter.
<i>realname</i>	String	Full user name.
<i>restart_background_jobs</i>	Boolean	Indicates whether to restart background search job that has not completed when the Splunk deployment restarts. <i>true</i> = Restart job. <i>false</i> = Do not restart job.
<i>roles</i>	String	Role to assign to this user. To assign multiple roles, pass in each role using a separate <i>roles</i> parameter value.

Name	Type	Description
		<p>For example, <code>-d roles="role1", -d roles="role2"</code>.</p> <p>At least one existing role is required if you are not using the <code>createrole</code> parameter to create a new role for the user. If you are using <code>createrole</code> to create a new role, you can optionally use this parameter to specify additional roles to assign to the user.</p>
<i>tz</i>	String	User timezone.

## Response keys

Name	Description
<i>capabilities</i>	List of capabilities assigned to role.
<i>defaultApp</i>	Default app for the user, which is invoked at login.
<i>defaultAppIsUserOverride</i>	<p>Default app override indicator.</p> <p><code>true</code> = Default app overrides the user role default app.</p> <p><code>false</code> = Default app does not override the user role default app.</p>
<i>defaultAppSourceRole</i>	Role that determines the default app for the user, if the user has multiple roles.
<i>email</i>	User email address.
<i>password</i>	User password.
<i>realname</i>	User full name.
<i>restart_background_jobs</i>	<p>Indicates whether to restart background search job that has not completed when the Splunk deployment restarts.</p> <p><code>true</code> = Restart job.</p> <p><code>false</code> = Do not restart job.</p>
<i>roles</i>	Roles assigned to the user.
<i>type</i>	<p>One of the following user authentication system types.</p> <ul style="list-style-type: none"> <li>• LDAP</li> <li>• Scripted</li> <li>• Splunk</li> <li>• System (reserved for system user)</li> </ul>
<i>tz</i>	User timezone.

## 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 capabilities.

### Request parameters

Pagination and filtering parameters can be used with this method.

### Response keys

Name	Description
<i>capabilities</i>	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_httppaths</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_wmicconf</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_httppaths</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/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
<i>capabilities</i>	For users with the <code>edit_roles</code> capability, lists all capabilities. For users with <code>edit_roles_grantable</code> , <code>edit_user</code> , and <code>grantableRoles</code> , 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:list>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
```



```

    <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
<i>capabilities</i>	List of capabilities assigned to role.
<i>cumulativeRTSrchJobsQuota</i>	Maximum number of concurrently running real-time searches for all role members. Warning message logged when limit is reached.
<i>cumulativeSrchJobsQuota</i>	Maximum number of concurrently running searches for all role members. Warning message logged when limit is reached.
<i>defaultApp</i>	The name of the app to use as the default app for this role.  A user-specific default app overrides this.
<i>imported_capabilities</i>	List of capabilities assigned to role made available from imported roles.
<i>imported_roles</i>	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.
<i>imported_rtSrchJobsQuota</i>	The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.  <i>imported_rtSrchJobsQuota</i> specifies the quota imported from other roles.
<i>imported_srchDiskQuota</i>	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.

Name	Description
	imported_srchDiskQuota specifies the quota for this role that have imported from other roles.
<i>imported_srchFilter</i>	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.
<i>imported_srchIndexesAllowed</i>	A list of indexes, imported from other roles, this role has permissions to search.
<i>imported_srchIndexesDefault</i>	A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.
<i>imported_srchJobsQuota</i>	The maximum number of historical searches for this role that are imported from other roles.
<i>imported_srchTimeWin</i>	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.
<i>rtSrchJobsQuota</i>	The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.
<i>srchDiskQuota</i>	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.
<i>srchFilter</i>	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.
<i>srchIndexesAllowed</i>	A list of indexes this role has permissions to search.
<i>srchIndexesDefault</i>	List of search indexes that default to this role when no index is specified.
<i>srchJobsQuota</i>	The maximum number of concurrent real time search jobs for this role.  This count is independent from the normal search jobs limit.
<i>srchTimeWin</i>	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_wmicnf</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:dict>
    </content>
  </entry>

```

```

    </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:list>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

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

```

```

    </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:list>
</s:key>

```

```

        <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:list>
            </s:key>
        </s:dict>
    </content>
</entry>

```

```

    <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
<i>capabilities</i>	String	List of capabilities assigned to role. To send multiple capabilities, send this argument multiple times.  Roles inherit all capabilities from imported roles.
<i>cumulativeRTSrchJobsQuota</i>	Number	Maximum number of concurrently running real-time searches that all members of this role can have.  <i>Note:</i> 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.
<i>cumulativeSrchJobsQuota</i>	Number	Maximum number of concurrently running searches for all role members. Warning message logged when limit is reached.  <i>Note:</i> 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.
<i>defaultApp</i>	String	Specify the folder name of the default app to use for this role. A user-specific default app overrides this.
<i>imported_roles</i>	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 <ul style="list-style-type: none"> <li>• admin</li> <li>• can_delete</li> <li>• power</li> <li>• user</li> </ul> You can specify additional roles created.
<i>name</i> required	String	<b>Required.</b> The name of the user role to create.

Name	Type	Description
<i>rtSrchJobsQuota</i>	Number	Specify the maximum number of concurrent real-time search jobs for this role.  This count is independent from the normal search jobs limit.
<i>srchDiskQuota</i>	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.
<i>srchFilter</i>	String	<p>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.</p> <p>The search string can include search fields and the following terms.</p> <ul style="list-style-type: none"> <li>• source</li> <li>• host</li> <li>• index</li> <li>• eventtype</li> <li>• sourcetype</li> <li>• *</li> <li>• OR</li> <li>• AND</li> </ul> <p>Example: "host=web* OR source=/var/log/*"</p> <p><b>Note:</b> You can also use the <i>srchIndexesAllowed</i> and <i>srchIndexesDefault</i> parameters to limit the search on indexes.</p>
<i>srchIndexesAllowed</i>	String	<p>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.</p> <p>Search indexes available by default include the following.</p> <ul style="list-style-type: none"> <li>• All internal indexes</li> <li>• All non-internal indexes</li> <li>• _audit</li> <li>• _blocksignature</li> <li>• _internal</li> <li>• _thefishbucket</li> <li>• history</li> <li>• main</li> </ul> <p>You can also specify other search indexes added to the server.</p>
<i>srchIndexesDefault</i>	String	<p>For this role, indexes to search when no index is specified.</p> <p>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".</p> <p>Search indexes available by default include the following.</p>

Name	Type	Description
		<ul style="list-style-type: none"> <li>• All internal indexes</li> <li>• All non-internal indexes</li> <li>• _audit</li> <li>• _blocksignature</li> <li>• _internal</li> <li>• _thefishbucket</li> <li>• history</li> <li>• main</li> <li>• other search indexes added to the server</li> </ul>
<i>srchJobsQuota</i>	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.
<i>srchTimeWin</i>	Number	<p>Maximum time span of a search, in seconds.</p> <p>By default, searches are not limited to any specific time window. To override any search time windows from imported roles, set <i>srchTimeWin</i> to '0', as the 'admin' role does.</p>

### 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"/>
</entry>
</s:messages>
</s:messages>
```

```

<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 following resource in *Securing Splunk Enterprise*. List of available capabilities

### 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:list>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

    <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
------	-------------

<i>capabilities</i>	List of capabilities assigned to this role.
<i>cumulativeRTSrchJobsQuota</i>	Maximum number of concurrently running real-time searches for all role members. A warning message is logged when this limit is reached.
<i>cumulativeSrchJobsQuota</i>	Maximum number of concurrently running searches for all role members. A warning message is logged when this limit is reached.
<i>defaultApp</i>	The name of the app to use as the default app for this role.  A user-specific default app overrides this.
<i>imported_capabilities</i>	List of capabilities assigned to role that were made available from imported roles.
<i>imported_roles</i>	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.
<i>imported_rtSrchJobsQuota</i>	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.  <i>imported_rtSrchJobsQuota</i> specifies the quota imported from other roles.
<i>imported_srchDiskQuota</i>	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.  <i>imported_rtSrchJobsQuota</i> specifies the quota imported from other roles.
<i>imported_srchFilter</i>	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.
<i>imported_srchIndexesAllowed</i>	A list of indexes, imported from other roles, this role has permissions to search.
<i>imported_srchIndexesDefault</i>	A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.
<i>imported_srchJobsQuota</i>	The maximum number of historical searches for this role that are imported from other roles.
<i>imported_srchTimeWin</i>	Maximum time span of a search, in seconds.  0 indicates searches are not limited to any specific time window.  <i>imported_srchTimeWin</i> specifies the limit from imported roles.
<i>rtSrchJobsQuota</i>	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.
<i>srchDiskQuota</i>	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.
<i>srchFilter</i>	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.
<i>srchIndexesAllowed</i>	A list of indexes this role has permissions to search.
<i>srchIndexesDefault</i>	List of search indexes that default to this role when no index is specified.

```

<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>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>srchJobsQuota</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: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>

```

**Name**

**Description**

```

<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>

```

## POST

Update the specified role.

### Request parameters

Name	Type	Description
<i>capabilities</i>	String	List of capabilities assigned to this role.
<i>cumulativeRTSrchJobsQuota</i>	Number	Maximum number of concurrently running real-time searches for all role members. A warning message is logged when this limit is reached.
<i>cumulativeSrchJobsQuota</i>	Number	Maximum number of concurrently running searches for all role members. A warning message is logged when this limit is reached.
<i>defaultApp</i>	String	The folder name for the app to use as the default app for this role. A user-specific default app overrides this.
<i>imported_capabilities</i>	String	List of capabilities assigned to role that were made available from imported roles.
<i>imported_roles</i>	String	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.
<i>imported_rtSrchJobsQuota</i>	String	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
		<i>imported_rtSrchJobsQuota</i> specifies the quota imported from other roles.
<i>imported_srchDiskQuota</i>	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.  <i>imported_rtSrchJobsQuota</i> specifies the quota imported from other roles.
<i>imported_srchFilter</i>	String	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.
<i>imported_srchIndexesAllowed</i>	String	A list of indexes, imported from other roles, this role has permissions to search.
<i>imported_srchIndexesDefault</i>	String	A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.
<i>imported_srchJobsQuota</i>	String	The maximum number of historical searches for this role that are imported from other roles.
<i>imported_srchTimeWin</i>	String	Maximum time span of a search, in seconds.  0 indicates searches are not limited to any specific time window.  <i>imported_srchTimeWin</i> specifies the limit from imported roles.
<i>rtSrchJobsQuota</i>	Number	The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.
<i>srchDiskQuota</i>	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.
<i>srchFilter</i>	String	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.
<i>srchIndexesAllowed</i>	String	A list of indexes this role has permissions to search.
<i>srchIndexesDefault</i>	String	List of search indexes that default to this role when no index is specified.
<i>srchJobsQuota</i>	Number	The maximum number of concurrent real time search jobs for this role.  This count is independent from the normal search jobs limit.
<i>srchTimeWin</i>	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/authorization/roles/newrole1 -d
defaultApp=launcher
```

## XML Response

```
<title>roles</title>
<id>https://localhost:8089/services/authorization/roles</id>
<updated>2014-06-30T13:33:38-07:00</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>2014-06-30T13:33:38-07:00</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">launcher</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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```



```

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

### 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:dict>
      </s:key>
    </s:dict>
  </content>
</link>

```

```

        <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
<i>name</i>	String	The user of the token. Can be up to 1024 characters.
<i>audience</i>	String	The purpose for the token. Can be up to 256 characters.
<i>expires_on</i>	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.  <i>Note:</i> If you specify <code>not_before</code> in addition to <code>expires_on</code> , <code>not_before</code> cannot be after <code>expires_on</code> ..
<i>not_before</i>	String	The time that the token becomes valid. Can be an absolute time or a relative time. This time cannot be in the past.  <i>Note:</i> If you specify <code>not_before</code> in addition to <code>expires_on</code> , <code>not_before</code> cannot be after <code>expires_on</code> ..

### 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[eyJraWQiOiJzcGxlbmsuc2VjcmV0IiwiaWxnIjoiaSFMlMTIiLCJ2ZXIiOiJ2MSIsInR0eXAiOiJzdGF0aWMifQ
.eyJpc3MiOiJhZG1pbmcm9tIGRvY3MtdW5peC00Iiwic3ViIjoiaXNlcjEyIiwiaWxkIjoiaXNlcjEiLCJpZHAiOiJzcGxlbmsiLCJqdGkiOiJhMWFmYTZhbnZqMjMzZmZlOTFhYjNlNTk3ODg5YjIwMTNjNTdjbWwMwUwNmE5Y2Y0ZTg2ZjgyODIxNDRIYTA5IiwiaWF0IjoxNTU2NDkwNDE
yLCJleHAiOiJAsIm5iciI6MTU1NjQ5MDQxMn0.KQhlN5bdiEPVB_m85VV3CVIA
_Ux5CI24AHoer6iElAbGLLPwvN0ntHsagUFyrhk6edvDofRvG6Z1o5F4NS8Cg]]></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:dict>
  </content>

```

```

<s:key name="headers">
  <s:dict>
    <s:key name="alg">HS512</s:key>
    <s:key name="kid">splunk.secret</s:key>
    <s:key name="typ">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
<i>name</i>	String	The user of the token. Can be up to 1024 characters.
<i>audience</i>	String	The purpose for the token. Can be up to 256 characters.
<i>expires_on</i>	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. <i>Note:</i> If you specify <i>not_before</i> in addition to <i>expires_on</i> , <i>not_before</i> cannot be after <i>expires_on</i> ..
<i>not_before</i>	String	The time that the token becomes valid. Can be an absolute time or a relative time. This time cannot be in the past. <i>Note:</i> If you specify <i>not_before</i> in addition to <i>expires_on</i> , <i>not_before</i> cannot be after <i>expires_on</i> ..

**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>

```





## 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 `admin_all_objects` 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
<i>clear_password</i>	Clear text password.
<i>encr_password</i>	Encrypted, stored password.
<i>password</i>	Password mask, always <code>*****</code> .
<i>realm</i>	Realm in which credentials are valid.
<i>username</i>	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
<i>name</i>	String	<b>Required.</b> Credentials username.
<i>password</i>	String	<b>Required.</b> Credentials user password.
<i>realm</i>	String	Credentials realm.

### Response keys

Name	Description
<i>encr_password</i>	Encrypted, stored password.
<i>password</i>	Password mask, always <b>*****</b> .
<i>realm</i>	Realm in which credentials are valid.
<i>username</i>	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 `admin_all_objects` 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
<i>clear_password</i>	Clear text password.

Name	Description
<i>encr_password</i>	Encrypted, stored password.
<i>password</i>	Password mask, always *****.
<i>realm</i>	Realm in which credentials are valid.
<i>username</i>	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
<i>password</i>	String	User password credential.

### Response keys

Name	Description
<i>clear_password</i>	Clear text password.
<i>encr_password</i>	Encrypted, stored password.
<i>password</i>	Password mask, always *****.
<i>realm</i>	Realm in which credentials are valid.



Name	Description
<i>username</i>	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 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**

Use the following URL for managed deployments. If necessary, submit a support case to open port 8089 on your deployment.

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

#### **Self-service Splunk Cloud deployments**

Use the following URL for self-service deployments. To get the required non-SAML user credentials, submit a support case.

```
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.

---

## 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>

```

```
</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
<i>author</i>	App author and optional contact information. For apps deployed on Splunkbase, the Splunkbase account username.
<i>check_for_updates</i>	Indicates whether to check for updates. <code>true</code> = Check Splunkbase for app updates. <code>false</code> = Do not check Splunkbase for app updates.
<i>configured</i>	Custom setup complete indication: <code>true</code> = Custom app setup complete. <code>false</code> = Custom app setup not complete.
<i>description</i>	App description.
<i>details</i>	URL to use for detailed information about the app.
<i>disabled</i>	App state indication. <code>true</code> = App is disabled. <code>false</code> = App is enabled.
<i>label</i>	App name.
<i>state_change_requires_restart</i>	Indicates whether to require restart on state change. <code>true</code> = App state change requires restart. <code>false</code> = App state change might not require restart depending on other restart requirements.
<i>version</i>	App version.
<i>visible</i>	Indicates whether app is visible and navigable from Splunk Web. <code>true</code> = App is visible and navigable. <code>false</code> = 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="alc9b18fdcf" 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"/>
  </entry>
</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:dict>
    </s:key>
  </s:dict>
</content type="text/xml">
```

```

        <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
<i>auth</i>	String	Splunkbase session token for operations like install and update that require login. Use <i>auth</i> or <i>session</i> when installing or updating an app through Splunkbase.
<i>author</i>	String	For apps posted to Splunkbase, use your Splunk account username. For internal apps, include your name and contact information.
<i>configured</i>	Boolean	Custom setup complete indication: <code>true</code> = Custom app setup complete. <code>false</code> = Custom app setup not complete.
<i>description</i>	String	Short app description also displayed below the app title in Splunk Web Launcher.
<i>explicit_appname</i>	String	Custom app name. Overrides <i>name</i> when installing an app from a file where <i>filename</i> is set to <code>true</code> . See also <i>filename</i> .
<i>filename</i>	Boolean	Indicates whether to use the <i>name</i> value as the app source location. <code>true</code> indicates that <i>name</i> is a path to a file to install. <code>false</code> indicates that <i>name</i> is the literal app name and that the app is created from Splunkbase using a template.
<i>label</i>	String	App name displayed in Splunk Web, from five to eighty characters excluding the prefix "Splunk for".
<i>name</i>	String	<b>Required.</b> Literal app name or path for the file to install, depending on the value of <i>filename</i> . <i>filename</i> = <code>false</code> indicates that <i>name</i> is the literal app name and that the app is created from Splunkbase using a

Name	Type	Description
		<p>template.</p> <p><i>filename</i> = <i>true</i> indicates that <i>name</i> is the URL or path to the local <i>.tar</i>, <i>.tgz</i> or <i>.spl</i> file. If <i>name</i> is the Splunkbase URL, set <i>auth</i> or <i>session</i> to authenticate the request.</p> <p>The app folder name cannot include spaces or special characters.</p>
<i>session</i>	String	Login session token for installing or updating an app on Splunkbase. Alternatively, use <i>auth</i> .
<i>template</i>	Enum	<p>App template to use when creating the app"</p> <p><i>barebones</i> - [Default] Basic app framework.</p> <p><i>sample_app</i> - Example views and searches.</p> <p>Any custom app template.</p>
<i>update</i>	Boolean	<p>File-based update indication:</p> <p><i>true</i> specifies that <i>filename</i> should be used to update an existing app. If not specified, <i>update</i> defaults to <i>false</i>, which indicates that <i>filename</i> should not be used to update an existing app.</p>
<i>version</i>	String	App version.
<i>visible</i>	Boolean	<p>Indicates whether the app is visible and navigable from Splunk Web.</p> <p><i>true</i> = App is visible and navigable.</p> <p><i>false</i> = App is not visible or navigable.</p>

## Response keys

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

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



```
    <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
<i>refresh</i>	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
<i>author</i>	For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.
<i>check_for_updates</i>	Indicates whether to check for updates. true = Check Splunkbase for app updates. false = Do not check Splunkbase for app updates.
<i>configured</i>	Custom setup completeness indication. true = Custom app setup complete. false = Custom app setup not complete.
<i>description</i>	Brief app description also displayed below the app title in Splunk Web.
<i>disabled</i>	App state indication: true = App is disabled. false = App is enabled.
<i>label</i>	App name displayed in Splunk Web, from five to 80 characters and excluding the prefix "Splunk For".
<i>state_change_requires_restart</i>	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.
<i>version</i>	App version.
<i>visible</i>	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
successor app to UI Examples 4.1+. Splunk Dashboard Examples contains over 50 examples updated for Splunk 5.
Each example contains inline documentation 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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
```

```

<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
------	------	-------------

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

## Response keys

Name	Description
<i>author</i>	For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.
<i>check_for_updates</i>	Check for updates indication: <code>true</code> = Check Splunkbase for app updates. <code>false</code> = Do not check Splunkbase for app updates.
<i>configured</i>	Custom setup completion indicator. <code>true</code> = Custom app setup complete. <code>false</code> = Custom app setup not complete.
<i>description</i>	App description also displayed below the app title in Splunk Web.
<i>disabled</i>	App state indication. <code>true</code> = App is disabled. <code>false</code> = App is enabled.
<i>label</i>	App name displayed in Splunk Web, from five to 80 characters and excluding the prefix "Splunk For".
<i>state_change_requires_restart</i>	Restart required on state change indication: <code>true</code> = App state change requires restart. <code>false</code> = App state change might not require restart, depending on other restart requirements.
<i>version</i>	App version.
<i>visible</i>	Indicator of whether app is visible and navigable from Splunk Web. <code>true</code> = App is visible and navigable. <code>false</code> = 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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

        </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

`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
<i>name</i>	App name and name of the folder containing the app.
<i>path</i>	Local path to an archive of the app.
<i>url</i>	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:dict>  
      </s:key>  
    </s:dict>  
  </content>  
</entry>  
</s:messages>  
</entry>  
</s:messages>
```

```
        </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.

## 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 indexer cluster nodes is not supported. For example, index cluster management endpoints are not applicable to Splunk Cloud deployments.

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

---

## 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
<i>cxn_timeout</i>	Low-level timeout, in seconds, for establishing connection between cluster nodes. Defaults to 60 seconds.
<i>disabled</i>	Indicates if this node is disabled.
<i>forwarderdata_rcv_port</i>	The port from which to receive data from a forwarder.
<i>forwarderdata_use_ssl</i>	Indicates whether to use SSL when receiving data from a forwarder.
<i>heartbeat_period</i>	Only valid for peer nodes in a cluster. The time, in seconds, that a peer attempts to send a heartbeat to the manager
<i>heartbeat_timeout</i>	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.
<i>manager_uri</i>	Valid only for nodes configured as a peer or searchhead.  URI of the cluster manager to which this node connects.
<i>max_peer_build_load</i>	The number of jobs that a peer can have in progress at any time that make the bucket searchable.
<i>max_peer_rep_load</i>	Maximum number of replications that can be ongoing as a target.
<i>mode</i>	Valid values: (manager   peer   searchhead   disabled) Defaults to disabled.  Sets operational mode for this cluster node. Only one manager may exist per cluster.
<i>ping_flag</i>	For internal use to facilitate communication between the manager and peers.
<i>quiet_period</i>	The time, in seconds, that a manager waits for peers to add themselves to the cluster.
<i>rcv_timeout</i>	Low-level timeout, in seconds, for receiving data between cluster nodes. Defaults to 60 seconds.
<i>register_forwarder_address</i>	Not used.  Reserved for future use.
<i>register_replication_address</i>	

Name	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.
<i>register_search_address</i>	IP address that advertises this indexer to search heads.
<i>rep_cxn_timeout</i>	Low-level timeout, in seconds, for establishing a connection for replicating data.
<i>rep_max_rcv_timeout</i>	Maximum cumulative time, in seconds, for receiving acknowledgement data from peers. Defaults to 600s.
<i>rep_max_send_timeout</i>	Maximum time, in seconds, for sending replication slice data between cluster nodes. Defaults to 600s.
<i>rep_rcv_timeout</i>	Low-level timeout, in seconds, for receiving data between cluster nodes.
<i>rep_send_timeout</i>	Low-level timeout, in seconds, for sending replication data between cluster nodes. Defaults to 5 seconds.
<i>replication_factor</i>	<p>Only valid for nodes configured as a manager.</p> <p>Determines how many copies of raw data are created in the cluster. This could be less than the number of cluster peers.</p> <p>Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.</p>
<i>replication_port</i>	TCP port to listen for replicated data from another cluster member.
<i>replication_use_ssl</i>	Indicates whether to use SSL when sending replication data.
<i>restart_timeout</i>	<p>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.</p> <p><i>Note:</i> This only works if the peer is restarted from Splunk Web.</p>
<i>search_factor</i>	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 <i>replication_factor</i> and greater than 0. Defaults to 2.
<i>secret</i>	<p>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.</p> <p>Corresponds to <i>pass4SymmKey</i> setting in <i>server.conf</i>.</p>
<i>send_timeout</i>	Low-level timeout, in seconds, for sending data between cluster nodes. Defaults to 60 seconds.
<i>summary_replication</i>	Boolean indicator of whether summary replication is on or off. A <code>true</code> 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
<i>available_sites</i>	N/A	Sets the various sites that are recognized for this manager. Valid values include <code>site1</code> to <code>site64</code> .
<i>cluster_label</i>	String	Label for this cluster.
<i>cxn_timeout</i>	Number	Low-level timeout, in seconds, for establishing connection between cluster nodes. Defaults to 60 seconds.
<i>heartbeat_period</i>	Number	Only valid for peer nodes in a cluster. Time, in seconds, that a peer attempts to send a heartbeat to the manager
<i>heartbeat_timeout</i>	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.
<i>manager_uri</i>	URI	Valid only for nodes configured as a peer or searchhead. URI of the cluster manager to which this node connects.
<i>max_peer_build_load</i>	Number	The number of jobs that a peer can have in progress at any time that make the bucket searchable.
<i>max_peer_rep_load</i>	Number	Maximum number of replications that can be ongoing as a target.
<i>mode</i>	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.
<i>multisite</i>	Boolean	Enable or disable the multisite feature for this cluster.
<i>notify_scan_period</i>	Non-zero number	Controls the frequency that the indexer scans summary folders for summary updates. Only used when <code>summary_replication</code> is enabled on the manager. Defaults to 10 seconds.
<i>ping_flag</i>	N/A	For internal use to facilitate communication between the manager and peers.
<i>quiet_period</i>	Number	The time, in seconds, that a manager waits for peers to add themselves to the cluster.
<i>rcv_timeout</i>	Number	Low-level timeout, in seconds, for receiving data between cluster nodes. Defaults to 60 seconds.
<i>register_forwarder_address</i>	N/A	Reserved for future use.
<i>register_replication_address</i>	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.

Name	Datatype	Description
<i>register_search_address</i>	N/A	IP address that advertises this indexer to search heads.
<i>rep_cxn_timeout</i>	Number	Low-level timeout, in seconds, for establishing a connection for replicating data.
<i>rep_max_rcv_timeout</i>	Number	Maximum cumulative time, in seconds, for receiving acknowledgement data from peers. Defaults to 600s.
<i>rep_max_send_timeout</i>	Number	Maximum time, in seconds, for sending replication slice data between cluster nodes. Defaults to 600s.
<i>rep_rcv_timeout</i>	Number	Low-level timeout, in seconds, for receiving data between cluster nodes.
<i>rep_send_timeout</i>	Number	Low-level timeout, in seconds, for sending replication data between cluster nodes. Defaults to 5 seconds.
<i>replication_factor</i>	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.
<i>replication_port</i>	Number	TCP port to listen for replicated data from another cluster member.
<i>replication_use_ssl</i>	Number	Indicates whether to use SSL when sending replication data.
<i>restart_timeout</i>	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.  <i>Note:</i> This only works if the peer is restarted from Splunk Web.
<i>search_factor</i>	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.
<i>secret</i>	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 <code>server.conf</code> .
<i>send_timeout</i>	Number	Low-level timeout, in seconds, for sending data between cluster nodes. Defaults to 60 seconds.
<i>site</i>	N/A	Site ID for peer/searchhead indexer. Valid values include <code>site1</code> to <code>site64</code> .
<i>site_replication_factor</i>	Number	Replication factor for a multisite configuration.
<i>site_search_factor</i>	Number	Search factor for a multisite configuration.
<i>summary_replication</i>	Boolean	Enable or disable summary replication.
<i>use_batch_mask_changes</i>	Boolean	Only valid for <code>mode=manager</code> . Specifies if the manager should process bucket mask changes in batch or individually one by one. Defaults to true. Set to false when there are 6.1 peers in the cluster for backwards compatibility.

### 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 <ul style="list-style-type: none"><li>StreamingSource</li><li>StreamingTarget</li><li>Complete</li><li>StreamingError</li><li>PendingTruncate Bucket is scheduled to truncate.</li><li>PendingDiscard Bucket is scheduled to discard.</li></ul>

Filter name	Datatype	Description
		<ul style="list-style-type: none"> <li>• <code>NonStreamingTarget</code></li> </ul>
<code>search_state</code>	String	Bucket search state. Available options are <ul style="list-style-type: none"> <li>• <code>Searchable</code></li> <li>• <code>Unsearchable</code></li> <li>• <code>PendingSearchable</code> Bucket scheduled to become searchable by transferring or building <code>tsidx</code> files.</li> <li>• <code>PendingUnsearchable</code> Bucket is scheduled to become unsearchable.</li> <li>• <code>SearchablePendingMask</code> Primary change is scheduled or in progress.</li> </ul>
<code>replication_count</code>	Number	Use <code>&lt;</code> , <code>&gt;</code> , <code>!=</code> or <code>=</code> with numbers to indicate filtering values.
<code>search_count</code>	Number	Use <code>&lt;</code> , <code>&gt;</code> , <code>!=</code> or <code>=</code> with numbers to indicate filtering values.
<code>bucket_size</code>	Number	Use <code>&lt;</code> , <code>&gt;</code> , <code>!=</code> or <code>=</code> with numbers to indicate filtering values.
<code>frozen</code>	Boolean <code>true</code>   <code>false</code>	Return frozen buckets or non-frozen buckets.
<code>has_primary</code>	Boolean <code>true</code>   <code>false</code>	Return buckets with primaries or without primaries.
<code>meets_multisite_replication_count</code>	Boolean <code>true</code>   <code>false</code>	Return buckets that meet cluster replication policy or buckets that do not meet cluster replication policy.
<code>meets_multisite_search_count</code>	Boolean <code>true</code>   <code>false</code>	Return buckets that meet cluster search policy or buckets that do not meet cluster search policy.
<code>multisite_bucket</code>	Boolean <code>true</code>   <code>false</code>	Return buckets created in multisite mode or buckets not created in multisite mode.
<code>origin_site</code>	String	Site of the indexer where buckets were created.
<code>standalone</code>	Boolean <code>true</code>   <code>false</code>	Use <code>true</code> or <code>1</code> to return standalone buckets. Use <code>false</code> or <code>0</code> to return clustered buckets.

Pagination and filtering parameters can be used with this method.

## Returned values

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

Name	Description
<i>standalone</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
</s:messages>
```

```

<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
<i>bucket_size</i>	Indicates the size, in bytes, of the bucket.
<i>constrain_to_origin_site</i>	Flag indicating this particular bucket is a clustered pre-multisite bucket. Such buckets are replicated only within their origin site.
<i>frozen</i>	Indicates if the bucket is frozen.
<i>index</i>	Name of the index to which the bucket belongs.
<i>origin_site</i>	Where the bucket originated.
<i>peers</i>	Lists information about buckets on peers to this manager.
<i>primaries_by_site</i>	Primary peer (GIUD).
<i>rep_count_by_site</i>	Number of buckets.
<i>search_count_by_site</i>	Number of searchable buckets.
<i>service_after_time</i>	Bucket service is deferred until after this time.
<i>standalone</i>	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](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}/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://localhost: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
<i>peer</i> (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
<i>index</i>	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
<i>peers</i> 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
<i>bucket_id</i>	String	N/A	<b>Required.</b> ID of bucket to update.
<i>peer</i>	GUID	N/A	<b>Required.</b> 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
<i>bucket_id</i>	String	N/A	<b>Required.</b> 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="b233a6clade2" 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="b233a6clade2" 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/apply

`https://<host>:<mPort>/services/cluster/manager/control/default/apply`  
Pushes a bundle.

## POST

Push a bundle.

### Request Parameters

Name	Type	Default	Description
<i>skip-validation</i>	Boolean	False	Set as true to skip the validation step for this bundle.
<i>ignore_identical_bundle</i>	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
<i>mode</i>	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
<i>level</i>	String	<b>Required.</b> Fixup priority level. Use one of the following level values, listed in order of priority. <ul style="list-style-type: none"><li>• <code>streaming</code> : Hot buckets that need to be rolled or have their size committed.</li><li>• <code>data_safety</code> : Buckets without at least two <code>rawdata</code> copies.</li><li>• <code>generation</code> : Buckets without a primary copy.</li><li>• <code>replication_factor</code> : Buckets without replication factor number of copies.</li><li>• <code>search_factor</code> : Buckets without search factor number of copies.</li><li>• <code>checksum_sync</code> : 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.</li></ul>
<i>index</i>	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
<code>id</code>	Bucket id.
<code>reason</code>	Initial or latest reason for the bucket being on this fixup level.
<code>timestamp</code>	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
<i>generation_id</i>	The ID for the current generation for this manager.
<i>generation_peers</i>	Lists the peers for this generation of the cluster.
<i>pending_generation_id</i>	The next generation ID used by the manager when committing a new generation. This value is useful for debugging.
<i>pending_last_attempt</i>	The timestamp of the last attempt to commit to the pending generation ID (if ever).
<i>pending_last_reason</i>	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
<i>name</i> required	String		The URI of the searchhead node of a cluster upon which to create a new generation.
<i>generation_poll_interval</i>	Number		How often, in seconds, the searchhead polls the manager for generation information.  Defaults to 60 seconds.
<i>label</i>	String		Server name for the Splunk platform instance specified by the <i>name</i> attribute.

Name	Type	Default	Description
<i>mgmt_port</i>	String		The management port of searchhead node in a cluster upon which you are creating a new generation.
<i>register_search_address</i>	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
<i>generation_id</i>	The ID for the current generation for this manager.
<i>generation_peers</i>	Lists the peers for this generation of the cluster.
<i>pending_generation_id</i>	The next generation ID used by the manager when committing a new generation.  This value is useful for debugging.
<i>pending_last_attempt</i>	The timestamp of the last attempt to commit to the pending generation ID (if ever).
<i>pending_last_reason</i>	The reason why this peer failed to commit to the pending generation.  This parameter is EMPTY if no such attempt was made.
<i>replication_factor_met</i>	Indicates if the replication factor was met for the cluster.
<i>search_factor_met</i>	Indicates if the search factor was met for the cluster.
<i>was_forced</i>	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
<i>generation_id</i>	The ID of the current generation for this manager.
<i>generation_peers</i>	Lists the peers for this generation of the cluster.
<i>pending_generation_id</i>	The next generation ID used by the manager when committing a new generation. This value is useful for debugging.
<i>pending_last_attempt</i>	The timestamp of the last attempt to commit to the pending generation ID (if ever).
<i>pending_last_reason</i>	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
<i>generation_poll_interval</i>	Number	How often, in seconds, the searchhead polls the manager for generation information.  Defaults to 60 seconds.
<i>label</i>	String	Server name for the search head specified by {name}.
<i>mgmt_port</i>	String	The managment port of searchhead node in a cluster upon which you are creating a new generation.
<i>register_search_address</i>	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 <code>splunkd</code> instance.

Returned values

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

Name	Description
<i>was_forced</i>	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/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
<i>all_data_is_searchable</i>	Boolean	Indicates if all data in the cluster is searchable.
<i>all_peers_are_up</i>	Boolean	Indicate if all peers are strictly in the Up status.
<i>cm_version_is_compatible</i>	Boolean	Indicates if any cluster peers are running a Splunk Enterprise version greater than or equal to the cluster manager's version.
<i>multisite</i>	Boolean	Indicates if multisite is enabled.
<i>no_fixups_in_progress</i>	Boolean	Indicates if there does not exist buckets with bucket state <code>NonStreamingTarget</code> , or bucket search states <code>PendingSearchable</code> or <code>SearchablePendingMask</code> .
<i>pre_flight_check</i>	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.
<i>replication_factor_met</i>	Boolean	

Name	Datatype	Description
		Only valid for mode=manager and multisite=false. Indicates whether the replication factor is met. If true, the cluster has at least <code>replication_factor</code> number of raw data copies in the cluster.
<code>search_factor_met</code>	Boolean	Only valid for mode=manager and multisite=false. Indicates whether the search factor is met. If true, the cluster has at least <code>search_factor</code> number of raw data copies in the cluster.
<code>site_replication_factor_met</code>	Boolean	Only valid for mode=manager and multisite=true. Indicates whether the site replication factor is met. If true, the cluster has at least <code>replication_factor</code> number of raw data copies in the cluster.
<code>site_search_factor_met</code>	Boolean	Only valid for mode=manager and multisite=true. Indicates whether the site search factor is met. If true, the cluster has at least <code>site_search_factor</code> number of raw data copies in the cluster.
<code>splunk_version_peer_count</code>	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="b233a6clade2" 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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

<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
<i>buckets_with_excess_copies</i>	Number of distinct buckets that have one or more excess replication copies.

Attribute	Description
<i>buckets_with_excess_searchable_copies</i>	Number of distinct buckets that have one or more excess searchable copies.
<i>index_size</i>	Size of the index
<i>is_searchable</i>	When every bucket in the index has a primary, the index is considered "searchable".
<i>non_site_aware_buckets_in_site_aware_cluster</i>	Number of buckets created when the cluster was not in a multisite config. (Included only when the cluster is in multisite config.)
<i>num_buckets</i>	Total number of distinct buckets.
<i>replicated_copies_tracker</i>	Displays how many distinct buckets have <i>X</i> number of copies. One of the following options.  actual_copies_per_slot Number of buckets with <i>X</i> copies.  expected_total_per_slot Expected number of buckets with <i>X</i> copies.
<i>searchable_copies_tracker</i>	Displays how many distinct buckets have <i>X</i> number of searchable copies. One of the following options.  actual_copies_per_slot Number of buckets with <i>X</i> searchable copies.  expected_total_per_slot Expected number of buckets with <i>X</i> searchable copies.
<i>sort_order</i>	Used by UI.
<i>total_excess_bucket_copies</i>	Total number of excess copies for all buckets.
<i>total_excess_searchable_copies</i>	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
<i>buckets_with_excess_copies</i>	Number of distinct buckets that have one or more excess replication copies.
<i>buckets_with_excess_searchable_copies</i>	Number of distinct buckets that have one or more excess searchable copies.
<i>index_size</i>	Size of the index
<i>is_searchable</i>	When every bucket in the index has a primary, the index is considered "searchable".
<i>non_site_aware_buckets_in_site_aware_cluster</i>	Number of buckets created when the cluster was not in a multisite config. (Included only when the cluster is in multisite config.)
<i>num_buckets</i>	Total number of distinct buckets. Displays how many distinct buckets have <i>X</i> number of copies. One of the following options.  actual_copies_per_slot Number of buckets with <i>X</i> copies.  expected_total_per_slot Expected number of buckets with <i>X</i> copies.
<i>searchable_copies_tracker</i>	Displays how many distinct buckets have <i>X</i> number of searchable copies. One of the following options.  actual_copies_per_slot Number of buckets with <i>X</i> searchable copies.  expected_total_per_slot Expected number of buckets with <i>X</i> searchable copies.
<i>sort_order</i>	Used by UI.
<i>total_excess_bucket_copies</i>	Total number of excess copies for all buckets.
<i>total_excess_searchable_copies</i>	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
<i>active_bundle</i>	Provides information about the active bundle for this manager.
<i>bundle_creation_time_on_manager</i>	The time, in epoch seconds, when the bundle was created on the manager.
<i>bundle_validation_errors_on_manager</i>	A list of bundle validation errors.
<i>bundle_validation_in_progress</i>	Indicates if bundle validation is in progress.
<i>bundle_validation_on_manager_succeeded</i>	Indicates whether the manager succeeded validating bundles.
<i>data_safety_buckets_to_fix</i>	Lists the buckets to fix for the completion of data safety.
<i>gen_commit_buckets_to_fix</i>	The buckets to be fixed before the next generation can be committed.
<i>indexing_ready_flag</i>	Indicates if the cluster is ready for indexing.

Name	Description
<i>initialized_flag</i>	Indicates if the cluster is initialized.
<i>label</i>	The name for the manager. Displayed in the Splunk Web manager page.
<i>latest_bundle</i>	The most recent information reflecting any changes made to the manager-apps configuration bundle.  In steady state, this is equal to <i>active_bundle</i> . If it is not equal, then pushing the latest bundle to all peers is in process (or needs to be started).
<i>maintenance_mode</i>	Indicates if the cluster is in maintenance mode.
<i>reload_bundle_issued</i>	Indicates if the bundle issued is being reloaded.
<i>rep_count_buckets_to_fix</i>	Number of buckets to fix on peers.
<i>rolling_restart_flag</i>	Indicates whether the manager is restarting the peers in a cluster.
<i>search_count_buckets_to_fix</i>	Number of buckets to fix to satisfy the search count.
<i>service_ready_flag</i>	Indicates whether the manager is ready to begin servicing, based on whether it is initialized.
<i>start_time</i>	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:dict>
</s:key>
<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:dict>
  </s:key>
</s:dict>
... 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:dict>
</s:key>
<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: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>
    </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
<i>active_bundle_id</i>	The ID of the configuration bundle currently being used by the manager.
<i>apply_bundle_status</i>	Bundle status enumeration.
<i>base_generation_id</i>	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.
<i>bucket_count</i>	Count of the number of buckets on this peer, across all indexes.
<i>bucket_count_by_index</i>	Count of the number of buckets by index on this peer.

Name	Description
<i>delayed_buckets_to_discard</i>	List of bucket IDs waiting to be discarded on this peer.
<i>fixup_set</i>	The set of buckets that need repair once you take the peer offline.
<i>heartbeat_started</i>	Flag indicating if this peer has started heartbeating.
<i>host_port_pair</i>	The host and port advertised to peers for the data replication channel.  Can be either of the form IP:port or hostname:port.
<i>is_searchable</i>	Flag indicating if this peer belongs to the current committed generation and is searchable.
<i>label</i>	The name for the peer. Displayed on the manager page.
<i>last_heartbeat</i>	Timestamp for last heartbeat recieved from the peer.
<i>latest_bundle_id</i>	The ID of the configuration bundle this peer is using.
<i>pending_job_count</i>	Used by the manager to keep track of pending jobs requested by the manager to this peer.
<i>primary_count</i>	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.
<i>primary_count_remote</i>	Number of buckets for which the peer is primary that are not in its local site.
<i>replication_count</i>	Number of replications this peer is part of, as either source or target.
<i>replication_port</i>	TCP port to listen for replicated data from another cluster member.
<i>replication_use_ssl</i>	Indicates whether to use SSL when sending replication data.
<i>search_state_counter</i>	Lists the number of buckets on the peer for each search state for the bucket.  Possible values for search state include:  Searchable Unsearchable
<i>site</i>	To which site the peer belongs.
<i>status</i>	Indicates the status of the peer.  Valid values are:  Up Pending AutomaticDetention ManualDetention-PortsEnabled ManualDetention Restarting ShuttingDown ReassigningPrimaries Decommissioning GracefulShutdown Stopped Down BatchAdding
<i>status_counter</i>	Lists the number of buckets on the peer for each bucket status.

Name	Description
	<p>Possible values for bucket status:</p> <p>Complete: complete (warm/cold) bucket</p> <p>NonStreamingTarget: target of replication for already completed (warm/cold) bucket</p> <p>PendingTruncate: bucket pending truncation</p> <p>PendingDiscard: bucket pending discard</p> <p>Standalone: bucket that is not replicated</p> <p>StreamingError: copy of streaming bucket where some error was encountered</p> <p>StreamingSource: streaming hot bucket on source side</p> <p>StreamingTarget: streaming hot bucket copy on target side</p> <p>Unset: uninitialized</p>

## Example request and response

### XML Request

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

### 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>2014-04-17T19:17:08+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>6</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>238C3311-F0A4-4A9B-97F0-53667CFFEEAB</title>
  <id>https://localhost:8089/services/cluster/manager/peers/238C3311-F0A4-4A9B-97F0-53667CFFEEAB</id>
  <updated>2014-04-17T19:17:08+00:00</updated>
  <link href="/services/cluster/manager/peers/238C3311-F0A4-4A9B-97F0-53667CFFEEAB" rel="alternate"/>
  <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:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</feed>
```

```

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

```

```

        <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
<i>list_buckets</i>	Boolean	Indicates whether to list the buckets for the peers to this manager.

### Returned values

Name	Description
<i>active_bundle_id</i>	The ID of the configuration bundle currently being used by the manager.
<i>apply_bundle_status</i>	Bundle status enumeration.
<i>base_generation_id</i>	<p>The initial bundle generation ID recognized by this peer. Any searches from previous generations fail.</p> <p>The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the manager.</p>
<i>bucket_count</i>	Count of the number of buckets on this peer, across all indexes.
<i>bucket_count_by_index</i>	Count of the number of buckets by index on this peer.
<i>delayed_buckets_to_discard</i>	List of bucket IDs waiting to be discarded on this peer.
<i>fixup_set</i>	The set of buckets that need repair once you take the peer offline.
<i>heartbeat_started</i>	Flag indicating if this peer has started heartbeating.



Name	Description
<i>host_port_pair</i>	The host and port advertised to peers for the data replication channel.  Can be either of the form IP:port or hostname:port.
<i>is_searchable</i>	Flag indicating if this peer belongs to the current committed generation and is searchable.
<i>label</i>	The name for the peer. Displayed on the Splunk Web manager page.
<i>last_heartbeat</i>	Timestamp for last heartbeat recieved from the peer.
<i>latest_bundle_id</i>	The ID of the configuration bundle this peer is using.
<i>pending_job_count</i>	Used by the manager to keep track of pending jobs requested by the manager to this peer.
<i>primary_count</i>	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.
<i>primary_count_remote</i>	Number of buckets for which the peer is primary that are not in its local site.
<i>replication_count</i>	Number of replications this peer is part of, as either source or target.
<i>replication_port</i>	TCP port to listen for replicated data from another cluster member.
<i>replication_use_ssl</i>	Indicates whether to use SSL when sending replication data.
<i>search_state_counter</i>	Lists the number of buckets on the peer for each search state for the bucket.  Possible values for search state include:  Searchable Unsearchable
<i>site</i>	To which site the peer belongs.
<i>splunk_version</i>	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.
<i>status</i>	Indicates the status of the peer.  Valid values are:  Up Pending AutomaticDetention ManualDetention-PortsEnabled ManualDetention Restarting ShuttingDown ReassigningPrimaries Decommissioning GracefulShutdown Stopped Down BatchAdding
<i>status_counter</i>	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

Name	Description
	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:dict>
  </content>
</entry>
</feed>
```

```

    </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/sites

`https://<host>:<mPort>/services/cluster/manager/sites`  
Access cluster site information.

### GET

List available cluster sites.

### Request parameters

None

### Returned values

Name	Description
<i>peers</i>	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
<i>peers</i>	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">slp3</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">slp2</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">slp1</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
<i>decommission_force_timeout</i>	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 <code>rolling_restart=searchable_force</code> . Default value is 180. Max accepted value is 1800.
<i>maintenance_mode</i>	Indicates if the cluster is in maintenance mode. Happens during rolling restart, bundle push, and other maintenance activities.
<i>messages</i>	Array of messages from server.
<i>multisite</i>	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.
<i>peers</i>	Object containing all the peers in the cluster. For each peer, the label, site and status are provided.
<i>restart_inactivity_timeout</i>	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 <code>rolling_restart=searchable_force</code> . Default is 600secs.
<i>restart_progress</i>	Object containing lists of peers in "done", "failed", "in_progress" and "to_be_restarted" state.
<i>rolling_restart_flag</i>	Boolean that indicates if there is a rolling restart in progress.
<i>rolling_restart_or_upgrade</i>	Boolean that indicates if there is a rolling restart or rolling upgrade in progress.
<i>searchable_rolling</i>	Boolean that indicates if a searchable rolling restart/upgrade in progress.
<i>service_ready_flag</i>	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="b233a6clade2" 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:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

        <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



```
</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
<i>generation_id</i>	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.
<i>generation_peers</i>	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
<i>name</i>	String	<b>Required.</b> The URI of the manager node in the cluster.
<i>secret</i>	String	<b>Required.</b> 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
<i>manager_uri</i>	String	The URI of the manager node in the cluster for which this searchhead is configured.
<i>secret</i>	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
<i>generation_id</i>	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
<i>checksum</i>	Used internally to identify this bucket.
<i>earliest_time</i>	Indicates the time of the earliest event in this bucket.
<i>generation_id</i>	The generation ID for this peer.
<i>generations</i>	A sparse list of generation id to bucket primacy for the given peer.
<i>latest_time</i>	Indicates the time for the latest event in this bucket.
<i>search_state</i>	Indicates if the bucket is <code>searchable</code> or <code>unsearchable</code> .

Name	Description
<i>status</i>	<p>Indicates the status of this bucket. One of the following values.</p> <p><b>Complete</b> The copy of this bucket contains the full complement of information.</p> <p><b>StreamingSource</b> The copy of this bucket is sending data to peer nodes for replication.</p> <p><b>StreamingTarget</b> The copy of this bucket is receiving replicated data.</p> <p><b>NonStreamingTarget</b> This copy of a warm bucket replication is in progress. Once replication is complete, the status changes to Complete.</p> <p><b>StreamingError</b> The copy of this bucket encountered errors while streaming data.</p> <p><b>PendingTruncate</b> The manager asked the peer to truncate this copy of the bucket to a certain size and is waiting for confirmation.</p> <p><b>PendingDiscard</b> The manager asked the peer to discard this copy of the bucket (for whatever reason, and is waiting for confirmation.</p> <p><b>Standalone</b> A bucket in the cluster that is not replicated.</p>

## 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
<i>bucket_id</i>	String	<b>Required.</b> 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
<i>generation_id</i>	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
<i>checksum</i>	Used internally to identify this bucket.
<i>earliest_time</i>	Indicates the time of the earliest event in this bucket.
<i>generation_id</i>	The generation ID for this peer.
<i>generations</i>	A sparse list of generation id to bucket primacy for the given peer.
<i>latest_time</i>	Indicates the time for the latest event in this bucket.
<i>search_state</i>	Indicates if the bucket is <code>Searchable</code> or <code>Unsearchable</code> .
<i>status</i>	Indicates the status of this bucket. One of the following values.  <div> <div>Complete</div> <div>The copy of this bucket contains the full complement of information.</div> </div> <div> <div>StreamingSource</div> <div>The copy of this bucket is sending data to peer nodes for replication.</div> </div> <div> <div>StreamingTarget</div> <div>The copy of this bucket is receiving replicated data.</div> </div> <div> <div>NonStreamingTarget</div> <div>This copy of a warm bucket replication is in progress. Once replication is complete, the status changes to Complete.</div> </div> <div> <div>StreamingError</div> <div>The copy of this bucket encountered errors while streaming data.</div> </div> <div> <div>PendingTruncate</div> <div>The manager asked the peer to truncate this copy of the bucket to a certain size and is waiting for confirmation.</div> </div> <div> <div>PendingDiscard</div> </div>

Name	Description
	<p>The manager asked the peer to discard this copy of the bucket (for whatever reason, and is waiting for confirmation.</p> <p>Standalone</p> <p>A bucket in the cluster that is not replicated.</p>

## 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="b233a6clade2" 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
<i>clearMasks</i>	Boolean. Use <code>true</code> or <code>false</code> .	<code>true</code>	Optional. Indicates whether the manager should reassign all primary bucket copies across all peers. The default <code>true</code> value prompts the manager to reassign all primary bucket copies across all peers. Use <code>false</code> 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. <ul style="list-style-type: none"><li>• off: <b>Default.</b> Remove the indexer from the detention state.</li><li>• 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.</li><li>• 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.</li></ul>	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
<i>status</i>	<p>Indicates the status of the peer. One of the following values.</p> <ul style="list-style-type: none"> <li>• Up</li> <li>• Down</li> <li>• Pending</li> <li>• Detention</li> <li>• Restarting</li> <li>• DecommAwaitingPeer</li> <li>• DecommFixingBuckets</li> <li>• Decommissioned</li> </ul>

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

```

<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
<i>bookmark</i>	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.
<i>check_share_baseline</i>	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.
<i>unpublished</i>	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
<i>check_share_baseline</i>	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.
<i>server_name</i>	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	All changes on this cluster member have been pushed to the captain. There are no unpublished changes on this member.

Name	Description
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	<p>This member might be out of sync with the captain if this message persists after several replication periods.</p> <p>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.</p>

## 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>
```

## 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
<i>remote_sids</i>	Bool	<b>Required.</b> Set this to true to return the searches that the captain is seeing. Will include adhoc searches on remote members.

Returned values

Name	Description
<i>artifact_size</i>	Artifact size, in bytes.
<i>origin_guid</i>	Guid of the origin peer where this artifact was created/search was run.
<i>peers</i>	Lists information about replicas of this artifact on members of this searchhead cluster.
<i>service_after_time</i>	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_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-888888888888" rel="alternate"/>
    <author>
```

```

    <name>system</name>
  </author>
  <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14_
_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_U0Etbm14_
_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:dict>
    <s:key name="service_after_time">0</s:key>
  </s:dict>
</content>
</entry>
<entry>
  <title>scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888
-888888888888</title>
  <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14_
_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_U0Etbm14_
_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_U0Etbm14__RMD5b9b800e209365567_at_1413387300_288_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD5b9b800e209365567_at_1413387300_288
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
        <name>system</name>
    </author>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD5b9b800e209365567_at_1413387300_288
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14_
_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_U0Etbm14_
_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:dict>
    </content>

```

```

        </s:key>
      </s:dict>
    </s:key>
    <s:key name="service_after_time">0</s:key>
  </s:dict>
</content>
</entry>
<entry>
  <title>scheduler__admin_U0Etbm14__RMD5b9b800e209365567_at_1413387600_289_88888888-8888-8888-8888
-888888888888</title>
  <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__
_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_U0Etbm14__RMD5b9b800e209365567_at_1413387600_289
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD5b9b800e209365567_at_1413387600_289
_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link
href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14__
_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_U0Etbm14__
_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: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
<i>artifact_size</i>	Artifact size, in bytes.
<i>origin_guid</i>	Guid of the origin peer where this artifact was created.
<i>peers</i>	Lists information about artifacts on members of this captain.
<i>service_after_time</i>	Artifact service is deferred until after this time.

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost: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
<i>searchable</i>	Boolean	Maintain high search availability during a rolling restart.
<i>force</i>	Boolean	Override health check failures to continue searchable rolling restart.
<i>decommission_search_jobs_wait_secs</i>	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:dict>
  </content>
</entry>
```

```

    </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
<i>elected_captain</i>	Time when the current captain was elected
<i>id</i>	Id of this SH cluster. This is used as the unique identifier for the Search Head Cluster in bundle replication and acceleration summary management.
<i>initialized_flag</i>	Indicates if the searchhead cluster is initialized.
<i>label</i>	The name for the captain. Displayed on the Splunk Web manager page.
<i>maintenance_mode</i>	Indicates if the cluster is in maintenance mode.
<i>min_peers_joined_flag</i>	Flag to indicate if more then replication_factor peers have joined the cluster.
<i>peer_scheme_host_port</i>	URI of the current captain.
<i>rolling_restart_flag</i>	Indicates whether the captain is restarting the members in a searchhead cluster.
<i>service_ready_flag</i>	Indicates whether the captain is ready to begin servicing, based on whether it is initialized.
<i>start_time</i>	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
<i>ATTEMPT_[n]</i>	<i>dispatch_time</i> - The UTC time of dispatch for the job <i>errmsg</i> - If the job failed, capturing the reason for failure <i>peer</i> - GUID of the member that the job was sent to <i>sid</i> - the search id of this attempt <i>success</i> - a boolean for success/failure of the job
<i>job_state</i>	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.
<i>saved_search</i>	The name of the saved-search from the associated <code>savedsearches.conf</code> file.
<i>savedsearchtype</i>	The scheduler manages three kinds of scheduled jobs, regular <code>savedsearch</code> for both realtime and historical, <code>autosummary</code> report acceleration build searches, and <code>tsidx</code> build searches.
<i>search_app</i>	The application in which the savedsearch was created.
<i>search_owner</i>	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="errmsg">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_U0Etbm14__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="errmsg">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_U0Etbm14__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">888888888-8888-8888-8888-888888888888</s:key>
        <s:key
name="sid">scheduler__admin_U0Etbm14__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
<i>ATTEMPT_[n]</i>	<i>dispatch_time</i> - The UTC time of dispatch for the job <i>errormsg</i> - If the job failed, capturing the reason for failure <i>peer</i> - GUID of the member that the job was sent to <i>sid</i> - the search id of this attempt <i>success</i> - a boolean for success/failure of the job
<i>job_state</i>	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.
<i>saved_search</i>	The name of the saved-search from the associated <code>savedsearches.conf</code> file.
<i>savedsearchtype</i>	The scheduler manages three kinds of scheduled jobs, regular <code>savedsearch</code> for both realtime and historical, <code>autosummary</code> report acceleration build searches, and <code>tsidx</code> <code>tsidx</code> build searches.
<i>search_app</i>	The application in which the savedsearch was created.
<i>search_owner</i>	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_12944444515"  
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
<i>adhoc_searchhead</i>	Flag to indicate if this member does not run scheduled searches.
<i>advertise_restart_required</i>	Flag to indicate if this peer advertised that it needed a restart.
<i>artifact_count</i>	Number of artifacts on this peer
<i>delayed_artifacts_to_discard</i>	List of artifacts waiting to be deleted from this peer.
<i>fixup_set</i>	N/A
<i>host_port_pair</i>	The host and management port advertised by this peer.
<i>kv_store_host_port</i>	Host and port of the kv store instance of this member.
<i>label</i>	The name for this member. Displayed on the Splunk Web manager page.
<i>last_heartbeat</i>	Timestamp for last heartbeat recieved from the peer
<i>peer_scheme_host_port</i>	URI of the current captain.
<i>pending_job_count</i>	Used by the captain to keep track of pending jobs requested by the captain to this member.
<i>replication_count</i>	Number of replications this peer is part of, as either source or target.
<i>replication_port</i>	TCP port to listen for replicated data from another cluster member.
<i>replication_use_ssl</i>	Indicates whether to use SSL when sending replication data.
<i>site</i>	N/A
<i>status</i>	Indicates the status of the member. Possible values are the following. <ul style="list-style-type: none"><li>• Up</li><li>• Pending</li><li>• AutomaticDetention</li><li>• ManualDetention-PortsEnabled</li></ul>

Name	Description
	<ul style="list-style-type: none"> <li>• ManualDetention</li> <li>• Restarting</li> <li>• ShuttingDown</li> <li>• ReassigningPrimaries</li> <li>• Decommissioning</li> <li>• GracefulShutdown</li> <li>• Stopped</li> <li>• Down</li> <li>• BatchAdding</li> </ul>
<i>status_counter</i>	<p>Lists the number of buckets on the peer for each bucket status. Possible values are the following.</p> <p>Complete Complete (warm/cold) bucket</p> <p>NonStreamingTarget Target of replication for already completed (warm/cold) bucket</p> <p>PendingTruncate Bucket pending truncation</p> <p>PendingDiscard Bucket pending discard</p> <p>Standalone Bucket that is not replicated</p> <p>StreamingError Copy of streaming bucket where some error was encountered</p> <p>StreamingSource Streaming hot bucket on source side</p> <p>StreamingTarget Streaming hot bucket copy on target side</p> <p>Unset Uninitialized</p>

## 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>888888888-8888-8888-8888-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/members/888888888-8888-8888-8888-888888888888</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:dict>
  </content>
</entry>

```

```

<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
<i>adhoc_searchhead</i>	Flag to indicate if this member does not run scheduled searches.
<i>advertise_restart_required</i>	Flag to indicate if this peer advertised that it needed a restart.
<i>artifact_count</i>	Number of artifacts on this peer.
<i>delayed_artifacts_to_discard</i>	List of artifacts waiting to be deleted from this peer.
<i>fixup_set</i>	N/A
<i>host_port_pair</i>	The host and management port advertised by this peer.
<i>kv_store_host_port</i>	Host and port of the kv store instance of this member.
<i>label</i>	The name for this member. Displayed on the Splunk Web manager page.

Name	Description
<i>last_heartbeat</i>	Timestamp for last heartbeat recieved from the peer
<i>peer_scheme_host_port</i>	URI of the current captain.
<i>pending_job_count</i>	Used by the manager to keep track of pending jobs requested by the manager to this peer.
<i>replication_count</i>	Number of replications this peer is part of, as either source or target.
<i>replication_port</i>	TCP port to listen for replicated data from another cluster member.
<i>replication_use_ssl</i>	Indicates whether to use SSL when sending replication data.
<i>site</i>	N/A
<i>status</i>	<p>Indicates the status of the member.</p> <p>Possible values are the following.</p> <ul style="list-style-type: none"> <li>• Up</li> <li>• Pending</li> <li>• AutomaticDetention</li> <li>• ManualDetention-PortsEnabled</li> <li>• ManualDetention</li> <li>• Restarting</li> <li>• ShuttingDown</li> <li>• ReassigningPrimaries</li> <li>• Decommissioning</li> <li>• GracefulShutdown</li> <li>• Stopped</li> <li>• Down</li> <li>• BatchAdding</li> </ul>
<i>status_counter</i>	<p>Lists the number of buckets on the peer for each bucket status. Possible values are the following.</p> <p>Complete Complete (warm/cold) bucket</p> <p>NonStreamingTarget Target of replication for already completed (warm/cold) bucket</p> <p>PendingTruncate Bucket pending truncation</p> <p>PendingDiscard Bucket pending discard</p> <p>Standalone Bucket that is not replicated</p> <p>StreamingError Copy of streaming bucket where some error was encountered</p> <p>StreamingSource Streaming hot bucket on source side</p> <p>StreamingTarget Streaming hot bucket copy on target side</p> <p>Unset Uninitialized</p>

## 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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

    <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 searchhead cluster node configuration.

GET

List searchhead cluster node configuration.

### Request parameters

Pagination and filtering parameters can be used with this method.

### Returned values

Name	Description
<i>cxn_timeout</i>	Low-level timeout, in seconds, for establishing connection between searchhead cluster nodes. Defaults to 60 seconds.
<i>disabled</i>	Indicates if this node is disabled.
<i>heartbeat_period</i>	Only valid for member nodes in a searchhead cluster. The time, in seconds, that a member attempts to send a heartbeat to the captain
<i>heartbeat_timeout</i>	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.
<i>id</i>	Id of the SH cluster this member is a part of.
<i>max_peer_rep_load</i>	Maximum number of replications that can be ongoing as a target.
<i>mode</i>	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.

Name	Description
<i>percent_peers_to_restart</i>	Percentage of peers to restart at the same time when doing a rolling restart.
<i>ping_flag</i>	For internal use to facilitate communication between the captain and members.
<i>quiet_period</i>	The time, in seconds, that a captain waits for members to add themselves to the searchhead cluster.
<i>rcv_timeout</i>	Low-level timeout, in seconds, for receiving data between searchhead cluster nodes. Defaults to 60 seconds.
<i>register_replication_address</i>	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.
<i>rep_cxn_timeout</i>	Low-level timeout, in seconds, for establishing a connection for replicating data.
<i>rep_max_rcv_timeout</i>	Maximum cumulative time, in seconds, for receiving acknowledgement data from members. Defaults to 600s.
<i>rep_max_send_timeout</i>	Maximum time, in seconds, for sending replication slice data between searchhead cluster nodes. Defaults to 600s.
<i>rep_rcv_timeout</i>	Low-level timeout, in seconds, for receiving data between searchhead cluster nodes.
<i>rep_send_timeout</i>	Low-level timeout, in seconds, for sending replication data between searchhead cluster nodes. Defaults to 5 seconds.
<i>replication_factor</i>	<p>Only valid for nodes configured as a captain.</p> <p>Determines how many copies of raw data are created in the searchhead cluster. This could be less than the number of searchhead cluster members.</p> <p>Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.</p>
<i>replication_port</i>	TCP port to listen for replicated data from another searchhead cluster member.
<i>replication_use_ssl</i>	Indicates whether to use SSL when sending replication data.
<i>restart_timeout</i>	<p>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.</p> <p>Note: This only works if the member is restarted from Splunk Web.</p>
<i>secret</i>	<p>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.</p> <p>Corresponds to <code>pass4SymmKey</code> setting in <code>server.conf</code>.</p>
<i>send_timeout</i>	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
<i>rolling_restart</i>	String	Sets the mode for search head cluster rolling restart. Options include: <ul style="list-style-type: none"><li>• <b>restart</b>: Initiates a rolling restart in classic mode (no guarantee of search continuity).</li><li>• <b>searchable</b>: Initiates a rolling restart with minimum search interruption.</li></ul>
<i>decommission_search_jobs_wait_secs</i>	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.
<i>manual_detention</i>	Use one of the following values: <ul style="list-style-type: none"><li>• <b>off</b>: Default. Remove the target search head from the detention state.</li><li>• <b>on</b>: Put the target search head in manual detention mode.</li></ul>	Specifies whether to put the cluster member in manual detention.
<i>target_uri</i>	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_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888
-888888888888</title>
    <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281
_88888888-8888-8888-8888-888888888888" rel="list"/>
    <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14__RMD5b9b800e209365567_at_1413387900_290_88888888-8888-8888-8888
-888888888888</title>
  <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD5b9b800e209365567_at_1413387900_290
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__RMD5b9b800e209365567_at_1413387900_290
_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14__RMD5b9b800e209365567_at_1413388200_291_88888888-8888-8888-8888
-888888888888</title>
  <id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14_
_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_U0Etbm14__RMD5b9b800e209365567_at_1413388200_291
_88888888-8888-8888-8888-888888888888" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__RMD5b9b800e209365567_at_1413388200_291
_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__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\_U0Etbm14\_\_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_U0Etbm14__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888</title>
  <id>https://wimpy.splunk.com:55569/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__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_U0Etbm14__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link
href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbm14__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
<i>manual_detention</i>	Use one of the following values.	Enable or disable manual detention.

Name	Type	Description
	<ul style="list-style-type: none"> <li>• <b>off: Default.</b> Remove the search head from the detention state.</li> <li>• <b>on:</b> Put the search head in manual detention mode.</li> </ul>	

### 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
<i>configuration_id</i>	Unique id for this configuration.
<i>servers_list</i>	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
<i>active_historical_search_count</i>	Number of currently running historical searches.
<i>active_realtime_search_count</i>	Number of currently running realtime searches.
<i>adhoc_searchhead</i>	Flag that indicates if this member can run scheduled searches.
<i>is_registered</i>	Indicates if this member is registered with the searchhead cluster captain.
<i>last_heartbeat_attempt</i>	Timestamp for the last attempt to contact the captain.
<i>maintenance_mode</i>	N/A
<i>peer_load_stats_gla_15m</i>	Number of scheduled searches run in the last 15 minutes.
<i>peer_load_stats_gla_1m</i>	Number of scheduled searches run in the last one minute.
<i>peer_load_stats_gla_5m</i>	Number of scheduled searches run in the last five minutes.
<i>peer_load_stats_max_runtime</i>	N/A
<i>peer_load_stats_num_autosummary</i>	N/A
<i>peer_load_stats_num_historical</i>	N/A
<i>peer_load_stats_num_realtime</i>	N/A
<i>peer_load_stats_num_running</i>	N/A
<i>peer_load_stats_total_runtime</i>	N/A
<i>restart_state</i>	Indicates whether the member needs to be restarted to enable its searchhead cluster configuration.
<i>status</i>	Indicates the status of the member. Possible values are as follows. <ul style="list-style-type: none"><li>• Up</li><li>• Pending</li><li>• AutomaticDetention</li><li>• ManualDetention</li><li>• Restarting</li><li>• ShuttingDown</li><li>• ReassigningPrimaries</li><li>• Decommissioning</li><li>• GracefulShutdown</li><li>• Down</li></ul>

## 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:dict>
    </content>
  </entry>
</feed>
```

```
</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
<i>advanced</i>	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	<i>decommission_search_jobs_wait_secs</i>	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.
	<i>dynamic_captain</i>	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
	<i>elected_captain</i>	String	The time when new captain is elected.
	<i>id</i>	String	Specifies the search head cluster GUID.
	<i>initialized_flag</i>	Boolean	Indicates if the captain is initialized.
	<i>label</i>	String	Specifies the search head cluster label.
	<i>max_failures_to_keep_majority</i>	Boolean	Indicates how many more nodes can be down to keep majority.
	<i>mgmt_uri</i>	String	Specifies the URI and management port for the captain.
	<i>min_peers_joined_flag</i>	Boolean	<i>min_peers_joined_flag</i> is true when there are at least as many search head peers as the replication_factor.
	<i>rolling_restart</i>	String	Shows the restart mode, either restart or searchable.
	<i>rolling_restart_flag</i>	Boolean	<i>rolling_restart_flag</i> is true when a rolling restart is in progress.
	<i>rolling_upgrade_flag</i>	Boolean	<i>rolling_upgrade_flag</i> is true when a rolling upgrade is in progress.
	<i>service_ready_flag</i>	Boolean	<i>service_ready_flag</i> is true when everything is up and running as expected and "ready to go!"
	<i>stable_captain</i>	Boolean	Indicates stable captain based on heartbeat.
Member	<i>label</i>	String	Specifies the search head label.
	<i>last_conf_replication</i>	String	Specifies when the member last pulled a set of configurations from the captain.
	<i>manual_detention</i>	Boolean	Indicates if the member is in manual detention.
	<i>mgmt_uri</i>	String	Specifies the URI and management port for the member.
	<i>mgmt_uri_alias</i>	String	Specifies the URI and management port for the member.
	<i>out_of_sync_node</i>	Boolean	<i>out_of_sync_node</i> is true when the member is out of sync.
	<i>preferred_captain</i>	Boolean	Indicates the member's preference for captaincy.
	<i>restart_required</i>	Boolean	<i>restart_required</i> is true when member requests a restart
	<i>splunk_version</i>	String	Splunk version running on the search head.
	<i>status</i>	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>
```

---

# 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 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.

---

## 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
<i>name</i>	String	<b>Required.</b> Stanza name in <code>{file}</code> configuration file.
<i>&lt;variable&gt;</i>	String	Arbitrary number of key/value pairs.

## 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:dict>
    </content>
  </entry>
</feed>
```

```

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

```

<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
<code>__conf</code>	String	<b>Required.</b> 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	<b>Required.</b> 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	<b>Required.</b> 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	<b>Required.</b> 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 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, deployment endpoints are not applicable to Splunk Cloud deployments.

See Using the REST API in Splunk Cloud in the *Splunk REST API Tutorials* 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
<i>disabled</i>	Disabled status: 0 = Enabled 1 = Disabled
<i>serverClasses</i>	List of member server classes for app download authorization.
<i>targetUri</i>	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
<i>disabled</i>	Disabled status: 0 = Enabled 1 = Disabled
<i>serverClasses</i>	List of member server classes for app download authorization.
<i>targetUri</i>	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
<i>disabled</i>	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 resource 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>
</s:messages>
</s:messages>
...
```

```
</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
<i>disabled</i>	Disabled status: 0 = Enabled 1 = Disabled
<i>serverClasses</i>	List of member server classes for app download authorization.
<i>targetUri</i>	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
<i>clientId</i>	String		Select apps that match <i>clientId</i> .
<i>hasDeploymentError</i>	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
<i>archive</i>	Disk location of the archived version of the app.
<i>clientId</i>	Deployment client ID associated with the app, an MD5 hash value of serialized (catenated) client attributes.

Name	Description
<i>hasDeploymentError</i>	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.
<i>loadtime</i>	Last deployment server app loaded or reloaded date and time. An application not mapped to <i>serverclasses</i> is not loaded so <i>loadtime</i> is 0.
<i>restartSplunkWeb</i>	Restart Splunk Web indication: 0 = Do not restart Splunk Web. 1 = Restart Splunk Web.
<i>restartSplunkd</i>	Restart splunkd indication: 0 = Do not restart splunkd. 1 = Restart splunkd.
<i>serverclasses</i>	List of server classes associated with the application.
<i>size</i>	Size on disk of the compressed app (bundle), in bytes.
<i>stateOnClient</i>	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:dict>
  </content>
</entry>
...

```

```

    <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
<i>archive</i>	Disk location of archived version of the app.
<i>clientId</i>	Deployment client ID associated with the app, an MD5 hash value of serialized (catenated) client attributes.
<i>hasDeploymentError</i>	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.
<i>loadtime</i>	Last deployment server app loaded or reloaded date and time. An application not mapped to <i>serverclasses</i> is not loaded so <i>loadtime</i> is 0.
<i>restartSplunkWeb</i>	Restart Splunk Web indication: 0 = Do not restart Splunk Web. 1 = Restart Splunk Web.
<i>restartSplunkd</i>	Restart splunkd indication: 0 = Do not restart splunkd. 1 = Restart splunkd.
<i>serverclasses</i>	List of server classes associated with the application.
<i>size</i>	Size on disk of the compressed app (bundle), in bytes.
<i>stateOnClient</i>	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
------	------	---------	-------------



<i>blacklist.*</i>	String		List of hosts to exclude when mapping application to a server class. For each <i>blacklist</i> , replace the wildcard (*) with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.
<i>continueMatching</i>	Boolean		Configuration layering indication, across classes and server-specific settings: <i>true</i> = [Default] Configuration lookups continue matching server classes after the first match. <i>false</i> = Use the first match, only.
<i>deinstall</i>	Boolean		Remove mapping indication: <i>true</i> = Remove mapping of {name} from all server classes and delete it from client target repositories. <i>false</i> = Do not remove mapping of {name}.
<i>filterType</i>	Enum		Filter execution order: <i>whitelist</i> = Whitelist filters are applied before blacklist filters. <i>blacklist</i> = Blacklist filters are applied before whitelist filters.
<i>machineTypesFilter</i>	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: <ul style="list-style-type: none"> <li>• You can specify '.' to mean '\.'</li> <li>• You can specify '*' to mean '.*'</li> <li>• Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.</li> </ul>
<i>repositoryLocation</i>	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
<i>restartSplunkWeb</i>	Boolean		Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated.  Defaults to false
<i>restartSplunkd</i>	Boolean		Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated.  Defaults to false
<i>serverclass</i>	String		The name of the server class to which the application is mapped.  Do not specify this parameter if <i>deinstall</i> is true.
<i>stateOnClient</i>	Enum		Valid values are (enabled   disabled   noop). <ul style="list-style-type: none"> <li>• <i>enabled</i>: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server.</li> <li>• <i>disabled</i>: Sets the application state to disabled on the client, regardless of state on the deployment server.</li> <li>• <i>noop</i>: The state on the client is the same as on the deployment server.</li> </ul>

Name	Type	Default	Description
<i>targetRepositoryLocation</i>	String		<p>The location on the deployment client to install the apps defined for this Deployment Server.</p> <p>If unset, or set to empty, the repositoryLocation path is used. That is, defaults to:</p> <p>\$SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk deployment)</p> <p>Useful only with complex (for example, tiered) deployment strategies.</p>
<i>tmpFolder</i>	String		<p>Working folder used by deployment server.</p> <p>Defaults to \$SPLUNK_HOME/var/run/tmp</p>
<i>unmap</i>	Boolean		Indicates whether to remove the mapping of the application to the specified server class.
<i>whitelist.*</i>	String		<p>List of hosts to accept for this server class.</p> <p>For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.</p>

## Returned values

Name	Description
<i>archive</i>	Specifies the location of the compressed version ( <i>bundle</i> ) of the app.
<i>blacklist.*</i>	<p>Regular expressions used to exclude, when mapping this application to a client.</p> <p>If a client matches any of the blacklist regular expressions, it does not receive the application. The * is replaced by an integral ordinal number.</p>
<i>continueMatching</i>	If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used.
<i>filterType</i>	<p>blacklist)</p> <p>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.</p> <p>See description for the filterType POST parameter for more information.</p>
<i>loadtime</i>	<p>Specifies the date and time the application was last loaded (or reloaded) by the deployment server.</p> <p>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.</p>
<i>machineTypesFilter</i>	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
<i>repositoryLocation</i>	The location on the deployment server to store the content that is to be deployed for this server class.
<i>restartSplunkWeb</i>	Indicates whether to restart Splunk Web.
<i>restartSplunkd</i>	Indicates whether to restart splunkd.

Name	Description
<i>serverclass</i>	The name of the server class to which the application is mapped.
<i>serverclasses</i>	List of server classes associated with the application.
<i>size</i>	Indicates in bytes the size on disk of the compressed version ( <i>bundle</i> ) of the application.
<i>stateOnClient</i>	Specifies whether the deployment client is enabled or disabled.
<i>targetRepositoryLocation</i>	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.
<i>tmpFolder</i>	Working folder used by deployment server.
<i>whitelist.*</i>	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:dict>
  </content>
</entry>
...

```

```

<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
<i>action</i>	String		Use one of the following values: <ul style="list-style-type: none"> <li>• <b>phonehome</b>: deployment client is verifying app status (typical state)</li> <li>• <b>unknown</b>: app state on deployment client restart</li> <li>• <b>download</b>: deployment client is downloading the app or app update</li> <li>• <b>install</b>: deployment client is installing or updating the app</li> <li>• <b>uninstall</b> app removed from deployment server, marked for uninstall on the deployment client</li> </ul> The GET response includes all clients with an app that has the specified action.
<i>application</i>	String		Lists clients to the deployment server that have attempted to download the named application.
<i>hasDeploymentError</i>	Boolean	False	Indicates whether to list only clients that have a deployment error.
<i>maxPhonehome_latency_to_avgInterval_ratio</i>	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.
<i>minLatestPhonehomeTime</i>	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)
<i>minPhonehome_latency_to_avgInterval_ratio</i>	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.
<i>serverclasses</i>	String		<p>Comma-separated list of serverclasses. List clients that are configured to receive an application to a listed serverclass.</p> <p>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.</p> <p>The "would have" is per blacklist.n or whitelist.n/machineTypesFilter in serverclass.conf</p>

Pagination and filtering parameters can be used with this method.

## Returned values

Name	Description
<i>applications</i>	List of applications deployed to the deployment client.
<i>averagePhoneHomeInterval</i>	The average phone home interval, in seconds.
<i>build</i>	The build number for the Splunk instance on the deployment client.
<i>dns</i>	The DNS lookup name of the deployment client server.
<i>guid</i>	Identifier for the deployment server client.
<i>hasDeploymentError</i>	Specifies whether to check for clients with a deployment error.
<i>hostname</i>	The host name of the deployment client server.
<i>id</i>	ID for the client based on client name and IP address.
<i>ip</i>	The IP address of the client to the deployment server.
<i>lastPhoneHomeTime</i>	The last time the deployment client phones home to the deployment server, in epoch time.
<i>mgmt</i>	The managment port for the deployment client.
<i>minLatestPhonehomeTime</i>	Specifies in epoch seconds the minimum latency for a client to contact the deployment server.
<i>minPhonehome_latency_to_avgInterval_ratio</i>	The minimum value specified for the ratio of the phone home latency to the average phone home interval.
<i>name</i>	The name of the deployment client server.
<i>serverclasses</i>	List of server classes for the deployment client.
<i>utsname</i>	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
<i>counts</i>	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
<i>application</i>	String		Count the number of downloads for clients that have attempted to download the named application.
<i>hasDeploymentError</i>	Boolean		Indicates whether to count downloads for clients that have a deployment error.
<i>maxAgeSecs required</i>	Number		Age of the downloads to count, in seconds.
<i>maxPhonehome_latency_to_avgInterval_ratio</i>	Number		List the count of recent download by this client 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
<i>minLatestPhonehomeTime</i>	Number		Specifies in epoch seconds the minimum latency for a client to contact the deployment server. This endpoint lists the number of downloads for clients to the deployment server with a latency equal to or greater than specified by this parameter.
<i>minPhonehome_latency_to_avgInterval_ratio</i>	Number		List the number of recent downloads by 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.

Name	Type	Default	Description
<i>serverclasses</i>	String		Comma-separated list of server classes. Lists the number of recent downloads by clients to the deployment server that are configured to send an application to a listed serverclass.

## Returned values

Name	Description
<i>count</i>	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
<i>application</i>	String		Lists information about this client with respect to the named application.
<i>hasDeploymentError</i>	Boolean		Indicates whether to list this client if has a deployment error.
<i>maxPhonehome_latency_to_avgInterval_ratio</i>	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.
<i>minLatestPhonehomeTime</i>	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.
<i>minPhonehome_latency_to_avgInterval_ratio</i>	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.
<i>serverclasses</i>	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
------	-------------

<i>application</i>	The name of the application specified to filter the results of this call.
<i>applications</i>	List of applications deployed to the deployment client.
<i>averagePhoneHomeInterval</i>	The average phone home interval, in seconds.
<i>build</i>	The build number for the Splunk instance on the deployment client.
<i>dns</i>	The DNS lookup name of the deployment client server.
<i>guid</i>	Identifier for the deployment server client.
<i>hasDeploymentError</i>	Specifies whether to check for clients with a deployment error.
<i>hostname</i>	The host name of the deployment client server.
<i>id</i>	ID for the client based on client name and IP address.
<i>ip</i>	The IP address of the client to the deployment server.
<i>lastPhoneHomeTime</i>	The last time the deployment client phones home to the deployment server, in epoch time.
<i>maxPhonehome_latency_to_avgInterval_ratio</i>	The maximum value specified for the ratio of the phone home latency to the average phone home interval.
<i>mgmt</i>	The management port for the deployment client.
<i>minLatestPhonehomeTime</i>	Specifies in epoch seconds the minimum latency for a client to contact the deployment server.
<i>minPhonehome_latency_to_avgInterval_ratio</i>	The minimum value specified for the ratio of the phone home latency to the average phone home interval.
<i>name</i>	The name of the deployment client server.
<i>serverClasses</i>	The list of server classes to which the client belongs.
<i>serverclasses</i>	List of server classes for the deployment client.
<i>utsname</i>	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:dict>
  </content>
</entry>

```

```

    <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
<i>currentDownloads</i>	The number of current downloads for this deployment server.
<i>disabled</i>	Indicates whether the deployment server is disabled.
<i>loadTime</i>	The time, in epoch seconds, the serverclass for this server was loaded.
<i>repositoryLocation</i>	The location on the deployment server to store the content that is to be deployed.
<i>whitelist.0</i>	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:dict>
  </content>
</entry>
</s:messages>
...
```



```
<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
<i>property</i>	The attribute that cannot be configured from Splunk Web.
<i>reason</i>	The reason an attribute cannot be configured from Splunk Web.
<i>stanza</i>	In Splunk Enterprise, the stanza in <code>serverclass.conf</code> 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
<i>disabled</i>	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
<i>blacklist-size</i>	The number of entires in the blacklist for this serverclass.

Name	Description
<i>clientId</i>	ID of deployment client for this server class.
<i>currentDownloads</i>	Number of applications currently downloaded.
<i>hasDeploymentError</i>	Indicates whether the serverclass has at least one deployment error.
<i>loadTime</i>	The time, in epoch seconds, this serverclass was loaded.
<i>machineTypesFilter</i>	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
<i>repositoryList</i>	List of applications stored at the location specified by repositoryLocation.
<i>repositoryLocation</i>	The location on the deployment server to store the content that is to be deployed for this server class.
<i>restartSplunkWeb</i>	Indicates whether to restart Splunk Web.
<i>restartSplunkd</i>	Indicates whether to restart splunkd.
<i>stateOnClient</i>	Indicates whether this server class is enabled or disabled.
<i>whitelist-size</i>	Specifies the number of entries in the whitelist for this server class.
<i>whitelist.0</i>	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/server/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/server/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
<i>name</i> required	String		The name of the server class.
<i>blacklist.*</i>	String		List of hosts to exclude for this server class.  For each blacklist, replace * with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.
<i>continueMatching</i>	Boolean		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.
<i>filterType</i>	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: <ul style="list-style-type: none"><li>• Items are not considered to match the server class by default.</li><li>• Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class.</li><li>• Items that match any blacklist entry are not considered to match the server class, regardless of whitelist.</li></ul> The blacklist setting indicates a filtering strategy that rules out a subset: <ul style="list-style-type: none"><li>• Items are considered to match the server class by default.</li><li>• Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class.</li><li>• Items that match any whitelist entry are considered to match the server class.</li></ul> 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

Name	Type	Default	Description
			you have to provide another filter in that server class definition to replace the one you overrode.
<i>machineTypesFilter</i>	String		<p>Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters.</p> <p>Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included.</p> <p>Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter.</p> <p>The patterns are PCRE regular expressions, with the following aids for easier entry:</p> <ul style="list-style-type: none"> <li>• You can specify '.' to mean '\\.'</li> <li>• You can specify '*' to mean '.*'</li> <li>• Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.</li> </ul>
<i>repositoryLocation</i>	String		<p>The location on the deployment server to store the content that is to be deployed for this server class.</p> <p>For example: \$SPLUNK_HOME/etc/deployment-apps</p>
<i>restartSplunkWeb</i>	Boolean		<p>Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated.</p> <p>Defaults to false</p>
<i>restartSplunkd</i>	Boolean		<p>Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated.</p> <p>Defaults to false</p>
<i>stateOnClient</i>	Enum		<p>Valid values are (enabled   disabled   noop).</p> <ul style="list-style-type: none"> <li>• <i>enabled</i>: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server.</li> <li>• <i>disabled</i>: Sets the application state to disabled on the client, regardless of state on the deployment server.</li> <li>• <i>noop</i>: The state on the client is the same as on the deployment server.</li> </ul>
<i>targetRepositoryLocation</i>	String		<p>The location on the deployment client to install the apps defined for this Deployment Server.</p> <p>If unset, or set to empty, the repositoryLocation path is used. That is, defaults to:</p> <p>\$SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk instance)</p> <p>Useful only with complex (for example, tiered) deployment strategies.</p>
<i>tmpFolder</i>	String		Working folder used by deployment server.

Name	Type	Default	Description
			Defaults to \$SPLUNK_HOME/var/run/tmp
<i>whitelist.*</i>	String		<p>List of hosts to accept for this server class.</p> <p>For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.</p>

#### Returned values

Name	Description
<i>blacklist-size</i>	The number of entries in the blacklist for this serverclass.
<i>blacklist.*</i>	<p>Regular expressions used to exclude for this server class.</p> <p>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.</p>
<i>continueMatching</i>	If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used.
<i>currentDownloads</i>	Number of applications currently downloaded.
<i>filterType</i>	<p>blacklist)</p> <p>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.</p> <p>See description for the filterType POST parameter for more information.</p>
<i>loadTime</i>	The time, in epoch seconds, this serverclass was loaded.
<i>machineTypesFilter</i>	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
<i>repositoryList</i>	List of applications stored at the location specified by repositoryLocation.
<i>repositoryLocation</i>	The location on the deployment server to store the content that is to be deployed for this server class.
<i>restartSplunkWeb</i>	Indicates whether to restart Splunk Web.
<i>restartSplunkd</i>	Indicates whether to restart splunkd.
<i>stateOnClient</i>	Specifies whether the deployment client is enabled or disabled.
<i>targetRepositoryLocation</i>	<p>The location on the deployment client to install the apps defined for this Deployment Server.</p> <p>If unset, or set to empty, the repositoryLocation path is used.</p> <p>That is, defaults to: \$SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk deployment.</p> <p>Useful only with complex (for example, tiered) deployment strategies.</p>
<i>tmpFolder</i>	<p>Working folder used by deployment server.</p> <p>Defaults to \$SPLUNK_HOME/var/run/tmp</p>
<i>whitelist-size</i>	Specifies the number of entries in the whitelist for this server class.



Name	Description
<i>whitelist.*</i>	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:dict>
  </content>
</entry>
</s:messages>
</s:messages>
```

```
<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
<i>newName</i> required	String		The new name of the server class.
<i>oldName</i> 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/server/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
<i>clientId</i>	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.
<i>hasDeploymentError</i>	Boolean		Indicates whether to only list server classes that have a deployment error.

### Returned values

Name	Description
<i>blacklist-size</i>	Specifies the size of the blacklist for the named server class.
<i>clientId</i>	ID of deployment client for this server class.
<i>currentDownloads</i>	The number of entires in the blacklist for this serverclass.
<i>hasDeploymentError</i>	Indicates whether the serverclass has at least one deployment error.
<i>loadTime</i>	The time, in epoch seconds, this serverclass was loaded.
<i>machineTypesFilter</i>	List of filters to be used in Boolean and logic with whitelist and blacklist filters.
<i>repositoryList</i>	List of applications stored at the location specified by repositoryLocation.
<i>repositoryLocation</i>	The location on the deployment server to store the content that is to be deployed for this server class.
<i>restartSplunkWeb</i>	Indicates whether to restart Splunk Web.
<i>restartSplunkd</i>	Indicates whether to restart splunkd.
<i>stateOnClient</i>	Indicates whether this server class is enabled or disabled.
<i>whitelist-size</i>	Specifies the number of entries in the whitelist for this server class.
<i>whitelist.0</i>	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/server/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
<i>blacklist.*</i>	String		List of hosts to exclude for this server class.  For each blacklist, replace * with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.
<i>continueMatching</i>	Boolean		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.
<i>filterType</i>	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: <ul style="list-style-type: none"><li>• Items are not considered to match the server class by default.</li><li>• Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class.</li><li>• Items that match any blacklist entry are not considered to match the server class, regardless of whitelist.</li></ul> The blacklist setting indicates a filtering strategy that rules out a subset: <ul style="list-style-type: none"><li>• Items are considered to match the server class by default.</li><li>• Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class.</li><li>• Items that match any whitelist entry are considered to match the server class.</li></ul> 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

Name	Type	Default	Description
			one you overrode.
<i>machineTypesFilter</i>	String		<p>Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters.</p> <p>Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included.</p> <p>Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter.</p> <p>The patterns are PCRE regular expressions, with the following aids for easier entry:</p> <ul style="list-style-type: none"> <li>• You can specify '.' to mean '\\.'</li> <li>• You can specify '*' to mean '.*'</li> <li>• Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.</li> </ul>
<i>repositoryLocation</i>	String		<p>The location on the deployment server to store the content that is to be deployed for this server class.</p> <p>For example: \$SPLUNK_HOME/etc/deployment-apps</p>
<i>restartSplunkWeb</i>	Boolean		<p>Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated.</p> <p>Defaults to false</p>
<i>restartSplunkd</i>	Boolean		<p>Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated.</p> <p>Defaults to false</p>
<i>stateOnClient</i>	Enum		<p>Valid values are (enabled   disabled   noop).</p> <ul style="list-style-type: none"> <li>• <i>enabled</i>: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server.</li> <li>• <i>disabled</i>: Sets the application state to disabled on the client, regardless of state on the deployment server.</li> <li>• <i>noop</i>: The state on the client is the same as on the deployment server.</li> </ul>
<i>targetRepositoryLocation</i>	String		<p>The location on the deployment client to install the apps defined for this Deployment Server.</p> <p>If unset, or set to empty, the repositoryLocation path is used. That is, defaults to:</p> <p>\$SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk instance)</p> <p>Useful only with complex (for example, tiered) deployment strategies.</p>
<i>tmpFolder</i>	String		<p>Working folder used by deployment server.</p> <p>Defaults to \$SPLUNK_HOME/var/run/tmp</p>



Name	Type	Default	Description
<i>whitelist.*</i>	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
<i>latest</i>	Boolean	Optional. If set to <code>true</code> , information about only the latest cycle is returned.

### Returned values

Name	Description
<code>bundle_id</code>	Knowledge bundle unique identifier composed of <code>hostname-creation_time</code>
<code>current_bundle</code>	Path to active knowledge bundle on disk
<code>current_repl_start_time</code>	Start time of current replication cycle
<code>cycle_id</code>	Bundle replication cycle unique identifier
<code>delta_path</code>	Path to the delta knowledge bundle on disk, if a delta was created
<code>is_repl_in_progress</code>	Boolean to indicate whether the replication cycle is in progress or completed
<code>peers_status</code>	Entry for each peer with <code>peer_name</code> and replication state for each peer
<code>replicationPolicy</code>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```
</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
<i>checksum</i>	Common checksum for entities in the bundle.
<i>filename</i>	Bundle file name
<i>location</i>	Bundle file path
<i>size</i>	Bundle size, in bytes
<i>timestamp</i>	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
<i>autoAddServers</i>	[Deprecated]
<i>blacklistNames</i>	List of filenames that match the blacklist pattern, and are not replicated.
<i>blacklistURLs</i>	List of URLs that are blacklisted, and thus is not replicated.
<i>checkTimedOutServersFrequency</i>	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 <i>removeTimedOutServers</i> is set to <code>true</code> . If <i>removeTimedOutServers</i> is <code>false</code> , this attribute is ignored.
<i>connectionTimeout</i>	Connection timeout.
<i>disabled</i>	Indicates if the distributed search is disabled.
<i>dist_search_enabled</i>	Indicates if the distributed search is enabled.
<i>heartbeatFrequency</i>	[Deprecated]
<i>heartbeatMcastAddr</i>	[Deprecated]
<i>heartbeatPort</i>	[Deprecated]
<i>receiveTimeout</i>	Amount of time in seconds to use as a timeout while trying to read/receive data from a search peer.
<i>removedTimedOutServers</i>	If true, removes a server connection that cannot be made within <i>serverTimeout</i> .  If false, every call to that server attempts to connect. This may result in a slow user interface.
<i>sendTimeout</i>	Send timeout.
<i>serverTimeout</i>	[Deprecated] Refer to <i>connectionTimeout</i> , <i>sendTimeout</i> , and <i>receiveTimeout</i> .
<i>servers</i>	The initial list of servers.  If operating completely in <i>autoAddServers</i> mode (discovering all servers), there is no need to list any servers here.
<i>shareBundles</i>	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."
<i>skipOurselves</i>	[Deprecated]

Name	Description
<i>statusTimeout</i>	Set connection timeout when gathering a search peer's basic info (/services/server/info). Read/write timeouts are automatically set to twice this value.
<i>ttr</i>	[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
<i>build</i>	The Splunk build number for this peer.
<i>bundle_versions</i>	The IDs of the bundles (of this search head) that the peer has. The IDs are sorted from latest to earliest.
<i>disabled</i>	Indicates if the peer is disabled.
<i>guid</i>	GUID of the peer.
<i>is_https</i>	Indicates if the management port is using SSL.
<i>licenseSignature</i>	The license signature.
<i>peerName</i>	The Splunk server name of the peer.
<i>peerType</i>	Specifies whether the peer is configured or discovered.
<i>replicationStatus</i>	The status of bundle replication to this peer. Can be any of the following values:  Initial In progress Failed Successful Mounted
<i>status</i>	The status of the peer.  Can be one of the following values:  Up

Name	Description
	Down Blacklisted Not a Splunk server Free Splunk server Authentication Failed Duplicate License Duplicate Servername Inconsistent bundles
<i>status_details</i>	Details of any errors encountered in the last heartbeat period.
<i>version</i>	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:dict>
  </content>
</entry>
...

```

```
<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
<i>name</i>	String			The name of the search peer.  Defined as hostname:port, where port is the management port.
<i>remotePassword</i>	String			The password of the remote user.
<i>remoteUsername</i>	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=myspass
```

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.

See About federated search for more 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 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 `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**.

#### *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 *Splunk REST API Tutorials* for more information.

---



## 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. See Define a federated provider.

### Authentication and authorization

Use of the GET and POST operations for this endpoint are restricted to roles that have the `admin_all_objects` and `indexes_edit capabilities`.

### 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	Description
<i>name</i>	Specifies the name of the federated provider.
<i>appContext</i>	<p>Specifies the Splunk application context for the federated searches that will be run with this federated provider definition. The application context ensures that federated searches using this federated provider are limited to the knowledge objects that are associated with the named application.</p> <p>If <code>useFSHKnowledgeObjects = true</code>, <code>appContext</code> specifies an app that is installed on the federated search head of your local Splunk platform deployment. If <code>useFSHKnowledgeObjects = false</code>, <code>appContext</code> specifies an app that is installed on the remote search head of the federated provider.</p>
<i>hostPort</i>	Specifies the protocols required to connect to a federated provider. Usually follows this format <code>&lt;Host_Name&gt;:&lt;Service_Port_Number&gt;</code> . In some cases, an IP address is used instead of a host name.
<i>serviceAccount</i>	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.
<i>type</i>	Specifies the federated provider type. At this point, only Splunk deployments are supported. Defaults to <code>splunk</code> .
<i>useFSHKnowledgeObjects</i>	<p>When set to <code>true</code>, specifies that federated searches with this provider use knowledge objects from the federated search head on the local deployment. When set to <code>false</code>, specifies that federated searches with this provider use knowledge objects from the remote deployment specified in the federated provider.</p> <p>Defaults to <code>True</code>.</p>

### Example request and response

Return a list of federated providers. (The XML response shows an example of a single returned federated provider record.)

### XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/federated/provider
```

### XML response

...

```

<entry>
  <title>provider-1</title>
  <id>/servicesNS/nobody/system/data/federated/provider/provider-1</id>
  <updated>1969-12-31T16:00:00-08:00</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"/>
  <link href="/servicesNS/nobody/system/data/federated/provider/provider-1/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="hostPort">localhost:8090</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>

```

POST

Creates a new federated provider definition.

### Request parameters

Name	Type	Description
------	------	-------------

<i>name</i>	String	<b>Required.</b> Specify a unique name for the federated provider.
<i>appContext</i>	String	<p>Specify the short name of an app to apply an application context to federated searches on the federated provider. The application context determines which set of knowledge objects is applied to the federated searches.</p> <ul style="list-style-type: none"> <li>• If <code>useFSHKnowledgeObjects = true</code>, provide the short name of an app that is installed on the federated search head of your local Splunk provider.</li> <li>• If <code>useFSHKnowledgeObjects = false</code>, provide the short name of an app that is installed on the remote search head of the federated provider.</li> </ul> <p>Defaults to <code>Search</code>.</p>
<i>hostPort</i>	String	<b>Required.</b> Provide the host name and port number for the federated provider, separated by a colon character. For example: <code>buttercupgames.splunkcloud.com:8089</code> .
<i>password</i>	String	<b>Required.</b> 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.
<i>serviceAccount</i>	String	<b>Required.</b> 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.
<i>type</i>	String	Set the type of federated provider. Currently only Splunk deployments are supported. Defaults to <code>splunk</code> . No other values are allowed.
<i>useFSHKnowledgeObjects</i>	Boolean	<p>When set to true, specifies that federated searches with this provider use knowledge objects from the federated search head on the local deployment. When set to false, specifies that federated searches with this provider use knowledge objects from the remote deployment specified in the federated provider.</p> <p>Defaults to <code>True</code>.</p>

## Returned values

Name	Description
<i>name</i>	Specifies the name of the federated provider.
<i>appContext</i>	<p>Specifies the Splunk application context for the federated searches that will be run with this federated provider definition. The application context ensures that federated searches using this federated provider are limited to the knowledge objects that are associated with the named application.</p> <p>If <code>useFSHKnowledgeObjects = true</code>, <code>appContext</code> specifies an app that is installed on the federated search head of your local Splunk platform deployment. If <code>useFSHKnowledgeObjects = false</code>, <code>appContext</code> specifies an app that is installed on the remote search head of the federated provider.</p>
<i>hostPort</i>	Specifies the protocols required to connect to a federated provider. Usually follows this format <code>&lt;Host_Name&gt;:&lt;Service_Port_Number&gt;</code> . In some cases, an IP address is used instead of a host name.
<i>serviceAccount</i>	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.
<i>type</i>	Specifies the federated provider type. At this point, only Splunk deployments are supported. Defaults to <code>splunk</code> .
<i>useFSHKnowledgeObjects</i>	<p>When set to true, specifies that federated searches with this provider use knowledge objects from the federated search head on the local deployment. When set to false, specifies that federated searches with this provider use knowledge objects from the remote deployment specified in the federated provider.</p> <p>Defaults to <code>True</code>.</p>

## Example request and response

Create a new definition for a federated provider named `provider-1`.

## XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/federated/provider -d name=provider-1 -d
type=splunk -d appContext=search -d hostPort=localhost:8090 -d serviceAccount=user1 -d password=secret1 -d
useFSHKnowledgeObjects=1
```

## XML response

```
...
<entry>
  <title>provider-1</title>
  <id>/servicesNS/nobody/system/data/federated/provider/provider-1</id>
  <updated>1969-12-31T16:00:00-08:00</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="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">localhost:8090</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>
```

## data/federated/provider/{federated\_provider\_name}

`https://<host>:<mPort>/services/data/federated/provider/{federated_provider_name}`

Use this endpoint to:

- Retrieve a definition for a specific {federated\_provider\_name}.
- Update a definition for a specific {federated\_provider\_name}.
- Delete a definition for a specific {federated\_provider\_name}.

See Define a federated provider.

### Authentication and Authorization

Usage of the GET, POST, and DELETE operations for this endpoint require the `admin_all_objects` and `indexes_edit capabilities`.

### GET

Returns a definition of a specific {federated\_provider\_name}.

### Request parameters

None specific to this method.

### Returned values

Name	Description
<i>name</i>	Specifies the name of the federated provider.
<i>appContext</i>	<p>Specifies the Splunk application context for the federated searches that will be run with this federated provider definition. The application context ensures that federated searches using this federated provider are limited to the knowledge objects that are associated with the named application.</p> <p>If <code>useFSHKnowledgeObjects = true</code>, <code>appContext</code> specifies an app that is installed on the federated search head of your local Splunk platform deployment. If <code>useFSHKnowledgeObjects = false</code>, <code>appContext</code> specifies an app that is installed on the remote search head of the federated provider.</p>
<i>hostPort</i>	Specifies the protocols required to connect to a federated provider. Usually follows this format <code>&lt;Host_Name&gt;:&lt;Service_Port_Number&gt;</code> . In some cases, an IP address is used instead of a host name.
<i>serviceAccount</i>	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.
<i>type</i>	Specifies the federated provider type. At this point, only Splunk deployments are supported. Defaults to <code>splunk</code> .
<i>useFSHKnowledgeObjects</i>	<p>When set to <code>true</code>, specifies that federated searches with this provider use knowledge objects from the federated search head on the local deployment. When set to <code>false</code>, specifies that federated searches with this provider use knowledge objects from the remote deployment specified in the federated provider.</p> <p>Defaults to <code>True</code>.</p>

### Example request and response

Return the definition for the `my_federated_provider` federated provider.

### XML Request

```
curl -k -u admin:changeme 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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

```

    </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">localhost:8090</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>

```

**POST**

Updates a definition for a specific {federated\_provider\_name}.

### Request parameters

At least one argument is required.

Name	Type	Description
<i>appContext</i>	String	<p>Specify the short name of an app to apply an application context to federated searches on the federated provider. The application context determines which set of knowledge objects is applied to the federated searches.</p> <ul style="list-style-type: none"> <li>• If <code>useFSHKnowledgeObjects = true</code>, provide the short name of an app that is installed on the federated search head of your local Splunk provider.</li> <li>• If <code>useFSHKnowledgeObjects = false</code>, provide the short name of an app that is installed on the remote search head of the federated provider.</li> </ul> <p>Defaults to <code>Search</code>.</p>
<i>hostPort</i>	String	<p>Provide the host name and port number for the federated provider, separated by a colon character. For example: <code>buttercupgames.splunkcloud.com:8089</code>.</p>
<i>password</i>	String	<p>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.</p>
<i>serviceAccount</i>	String	<p>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.</p>
<i>type</i>	String	<p>Set the type of federated provider. Currently only Splunk deployments are supported. Defaults to <code>splunk</code>. No other values are allowed.</p>
<i>useFSHKnowledgeObjects</i>	Boolean	<p>When set to true, specifies that federated searches with this provider use knowledge objects from the federated search head on the local deployment. When set to false, specifies that federated searches with this provider use knowledge objects from the remote deployment specified in the federated provider.</p> <p>Defaults to <code>True</code>.</p>

### Returned values

Name	Description
<i>name</i>	Specifies the name of the federated provider.
<i>appContext</i>	Specifies the Splunk application context for the federated searches that will be run with this federated provider definition. The application context ensures that federated searches using this federated provider are limited to the knowledge objects that are associated with the named application.  If <code>useFSHKnowledgeObjects = true</code> , <code>appContext</code> specifies an app that is installed on the federated search head of your local Splunk platform deployment. If <code>useFSHKnowledgeObjects = false</code> , <code>appContext</code> specifies an app that is installed on the remote search head of the federated provider.
<i>hostPort</i>	Specifies the protocols required to connect to a federated provider. Usually follows this format <code>&lt;Host_Name&gt;:&lt;Service_Port_Number&gt;</code> . In some cases, an IP address is used instead of a host name.
<i>serviceAccount</i>	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.
<i>type</i>	Specifies the federated provider type. At this point, only Splunk deployments are supported. Defaults to <code>splunk</code> .
<i>useFSHKnowledgeObjects</i>	When set to true, specifies that federated searches with this provider use knowledge objects from the federated search head on the local deployment. When set to false, specifies that federated searches with this provider use knowledge objects from the remote deployment specified in the federated provider.  Defaults to <code>True</code> .

### Example request and response

Change the `useFSHKnowledgeObjects` setting to `false` so that federated searches with this federated provider use knowledge objects from the remote search head on the provider.

### XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/federated/provider/my_federated_provider -d useFSHKnowledgeObjects=0
```

### 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="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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```



```

    <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="serviceAccount">power01</s:key>
<s:key name="type">splunk</s:key>
<s:key name="useFSHKnowledgeObjects">0</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 request and response

Remove the `my_federated_provider` stanza from `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>

```

## 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. See [Create a federated index](#).

### Authentication and authorization

Use of the GET and POST operations for this endpoint are 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 returned by this endpoint see the entry for `data/indexes`.

Name	Description
<i>name</i>	Specifies the name of the federated index. Uses the syntax <code>federated:&lt;index_name&gt;</code> .
<i>federated.provider</i>	Specifies the federated provider that contains the dataset to which this federated index maps.
<i>federated.dataset</i>	Specifies the dataset on the <code>federated.provider</code> to which this federated index maps. Each federated index maps to one dataset on a federated provider. The dataset is identified by its type and name, using the following syntax: <code>&lt;type&gt;:&lt;dataset_name&gt;</code> .

### Example request and response

Get the complete list of federated indexes. (The XML response provides a sample of one returned index record.)

### XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/federated/index
```

### XML response

```

...
<entry>
  <title>federated: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:airlinedata</s:key>
    <s:key name="federated.provider">remote_splunk_deployment</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>
POST

```

Creates a new federated index definition.

## Request parameters

Name	Type	Description
<i>name</i>	String	<p><b>Required.</b> Specify a unique name for the federated index, using the syntax <code>federated:&lt;index_name&gt;</code>. Each federated index maps to only one remote dataset on a federated provider, so the name should reference that dataset.</p> <p>Index names have the following limitations:</p> <ul style="list-style-type: none"> <li>• They may contain only lowercase letters, numbers, underscores, and hyphens.</li> <li>• They must begin with a letter or number.</li> </ul>

Name	Type	Description
		<ul style="list-style-type: none"> <li>• They cannot be more than 2048 characters in length.</li> <li>• They cannot contain the string "kvstore".</li> </ul>
<i>federated.provider</i>	String	<b>Required.</b> Specify the federated provider that contains the dataset to which this federated index maps.
<i>federated.dataset</i>	String	<b>Required.</b> Specify the dataset on the <i>federated.provider</i> to which this federated index maps. The dataset is identified by its type and name, using the following syntax: <code>&lt;type&gt;:&lt;dataset_name&gt;</code> .  For this version of the Splunk platform, the <code>&lt;type&gt;</code> is limited to <code>index</code> .

### Returned values

This table is limited to settings specific to federated indexes. For descriptions of other index settings returned by this endpoint see the entry for `data/indexes`.

Name	Description
<i>name</i>	Specifies the name of the federated index. Uses the syntax <code>federated:&lt;index_name&gt;</code> .
<i>federated.provider</i>	Specifies the federated provider that contains the dataset to which this federated index maps.
<i>federated.dataset</i>	Specifies the dataset on the <i>federated.provider</i> to which this federated index maps. Each federated index maps to one dataset on a federated provider. The dataset is identified by its type and name, using the following syntax: <code>&lt;type&gt;:&lt;dataset_name&gt;</code> .

### Example request and response

Create a new definition for a federated index named `airports-east`.

#### XML Request

```
curl -k -u admin:changeme 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:dict>
  </content>
</entry>
```

```

<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>

```

## data/federated/index/federated:{federated\_index\_name}

[https://<host>:<mPort>/services/data/federated/provider/federated:{federated\\_index\\_name}](https://<host>:<mPort>/services/data/federated/provider/federated:{federated_index_name})

Use this endpoint to:

- Retrieve a definition for a specific {federated\_index\_name}.
- Update a definition for a specific {federated\_index\_name}.
- Delete a definition for a specific {federated\_index\_name}.

See [Create a federated index](#).

### Authentication and Authorization

Usage of the GET, POST, and DELETE operations for this endpoint require the `admin_all_objects` and `indexes_edit` capabilities.

### GET

Returns a definition of a specific {federated\_index\_name}.

### Request parameters

None specific to this method.

### Returned values

This table is limited to settings specific to federated indexes. For descriptions of other index settings returned by this endpoint see the entry for [data/indexes](#).

Name	Description
<i>name</i>	Specifies the name of the federated index. Uses the syntax <code>federated:&lt;index_name&gt;</code> .

Name	Description
<i>federated.provider</i>	Specifies the federated provider that contains the dataset to which this federated index maps.
<i>federated.dataset</i>	Specifies the dataset on the <i>federated.provider</i> to which this federated index maps. Each federated index maps to one dataset on a federated provider. The dataset is identified by its type and name, using the following syntax: <type>:<dataset_name>.

### Example request and response

Return the definition for the `airports-east` federated index. **XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/data/federated/index/federated:airports-east
```

### XML response

```
<entry>
  <title>federated:airports-east</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east</id>
  <updated>1970-01-01T00:00:00+00:00</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="archiver.enableDataArchive">0</s:key>
      <s:key name="archiver.maxDataArchiveRetentionPeriod">0</s:key>
      <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="bucketRebuildMemoryHint">auto</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="eai:attributes">
    <s:dict>
        <s:key name="optionalFields">
            <s:list>
                <s:item>federated.dataset</s:item>
                <s:item>federated.provider</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="enableDataIntegrityControl">0</s:key>
<s:key name="enableOnlineBucketRepair">1</s:key>
<s:key name="enableRealtimeSearch">1</s:key>
<s:key name="enableTsidxReduction">0</s:key>
<s:key name="federated.dataset">sendmail</s:key>
<s:key name="federated.provider">remote_deployment_1</s:key>
<s:key name="fileSystemExecutorWorkers">5</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">10</s:key>
<s:key name="indexThreads">auto</s:key>
<s:key name="journalCompression">gzip</s:key>
<s:key name="maxBloomBackfillBucketAge">30d</s:key>
<s:key name="maxBucketSizeCacheEntries">0</s:key>
<s:key name="maxConcurrentOptimizes">6</s:key>
<s:key name="maxDataSize">auto</s:key>
<s:key name="maxGlobalDataSizeMB">0</s:key>
<s:key name="maxGlobalRawDataSizeMB">0</s:key>
<s:key name="maxHotBuckets">auto</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">8</s:key>
<s:key name="maxRunningProcessGroupsLowPriority">1</s:key>
<s:key name="maxTimeUnreplicatedNoAcks">300</s:key>
<s:key name="maxTimeUnreplicatedWithAcks">60</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">auto</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="minRawFileSyncSecs">disable</s:key>
<s:key name="minStreamGroupQueueSize">2000</s:key>
<s:key name="partialServiceMetaPeriod">0</s:key>
<s:key name="processTrackerServiceInterval">1</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="repFactor">0</s:key>
<s:key name="rotatePeriodInSecs">60</s:key>
<s:key name="rtRouterQueueSize">10000</s:key>
<s:key name="rtRouterThreads">0</s:key>
<s:key name="selfStorageThreads">2</s:key>
<s:key name="serviceInactiveIndexesPeriod">60</s:key>
<s:key name="serviceMetaPeriod">25</s:key>
<s:key name="serviceOnlyAsNeeded">1</s:key>
<s:key name="serviceSubtaskTimingPeriod">30</s:key>
<s:key name="splitByIndexKeys"></s:key>
<s:key name="streamingTargetTsidxSyncPeriodMsec">5000</s:key>
<s:key name="suppressBannerList"></s:key>
<s:key name="suspendHotRollByDeleteQuery">0</s:key>
<s:key name="sync">0</s:key>
<s:key name="syncMeta">1</s:key>
<s:key name="throttleCheckPeriod">15</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">2</s:key>
<s:key name="tstatsHomePath">volume:_splunk_summaries/$_index_name/datamodel_summary</s:key>
<s:key name="waitPeriodInSecsForManifestWrite">60</s:key>
<s:key name="warmToColdScript"></s:key>
</s:dict>
</content>
</entry>
POST

```

Updates a definition for a specific {federated\_index\_name}.

## Request parameters

At least one argument is required.

Name	Type	Description
<i>federated.provider</i>	String	<b>Required.</b> Specify the federated provider that contains the dataset to which this federated index maps.

Name	Type	Description
<i>federated.dataset</i>	String	<b>Required.</b> Specify the dataset on the <code>federated.provider</code> to which this federated index maps. The dataset is identified by its type and name, using the following syntax: <code>&lt;type&gt;:&lt;dataset_name&gt;</code> .  For this version of the Splunk platform, the <code>&lt;type&gt;</code> is limited to <code>index</code> .

### Returned values

This table is limited to settings specific to federated indexes. For descriptions of other index settings returned by this endpoint see the entry for `data/indexes`.

Name	Description
<i>name</i>	Specifies the name of the federated index. Uses the syntax <code>federated:&lt;index_name&gt;</code> .
<i>federated.provider</i>	Specifies the federated provider that contains the dataset to which this federated index maps.
<i>federated.dataset</i>	Specifies the dataset on the <code>federated.provider</code> to which this federated index maps. Each federated index maps to one dataset on a federated provider. The dataset is identified by its type and name, using the following syntax: <code>&lt;type&gt;:&lt;dataset_name&gt;</code> .

### Example request and response

Update the dataset mapping for the `federated:airports-east` federated index.

### XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/federated/index/federated:airports-east -d federated.dataset=index:airports-west
```

### XML response

```
<entry>
  <title>federated:airports-east</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/federated/index/federated%3Aairports-east</id>
  <updated>1970-01-01T00:00:00+00:00</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="archiver.enableDataArchive">0</s:key>
      <s:key name="archiver.maxDataArchiveRetentionPeriod">0</s:key>
      <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="bucketRebuildMemoryHint">auto</s:key>
      <s:key name="coldPath.maxDataSizeMB">0</s:key>
      <s:key name="coldToFrozenDir"></s:key>
    </s:dict>
  </content>
</entry>
```

```

<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="enableOnlineBucketRepair">1</s:key>
<s:key name="enableRealtimeSearch">1</s:key>
<s:key name="enableTsidxReduction">0</s:key>
<s:key name="federated.dataset">index:airports-west</s:key>
<s:key name="federated.provider">remote_deployment_1</s:key>
<s:key name="fileSystemExecutorWorkers">5</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">10</s:key>
<s:key name="indexThreads">auto</s:key>
<s:key name="journalCompression">gzip</s:key>
<s:key name="maxBloomBackfillBucketAge">30d</s:key>
<s:key name="maxBucketSizeCacheEntries">0</s:key>
<s:key name="maxConcurrentOptimizes">6</s:key>
<s:key name="maxDataSize">auto</s:key>
<s:key name="maxGlobalDataSizeMB">0</s:key>
<s:key name="maxGlobalRawDataSizeMB">0</s:key>
<s:key name="maxHotBuckets">auto</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">8</s:key>
<s:key name="maxRunningProcessGroupsLowPriority">1</s:key>
<s:key name="maxTimeUnreplicatedNoAcks">300</s:key>
<s:key name="maxTimeUnreplicatedWithAcks">60</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">auto</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="minRawFileSyncSecs">disable</s:key>
<s:key name="minStreamGroupQueueSize">2000</s:key>
<s:key name="partialServiceMetaPeriod">0</s:key>
<s:key name="processTrackerServiceInterval">1</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="repFactor">0</s:key>
<s:key name="rotatePeriodInSecs">60</s:key>
<s:key name="rtRouterQueueSize">10000</s:key>
<s:key name="rtRouterThreads">0</s:key>
<s:key name="selfStorageThreads">2</s:key>
<s:key name="serviceInactiveIndexesPeriod">60</s:key>
<s:key name="serviceMetaPeriod">25</s:key>
<s:key name="serviceOnlyAsNeeded">1</s:key>
<s:key name="serviceSubtaskTimingPeriod">30</s:key>
<s:key name="splitByIndexKeys"></s:key>
<s:key name="streamingTargetTsidxSyncPeriodMsec">5000</s:key>
<s:key name="suppressBannerList"></s:key>
<s:key name="suspendHotRollByDeleteQuery">0</s:key>
<s:key name="sync">0</s:key>
<s:key name="syncMeta">1</s:key>
<s:key name="throttleCheckPeriod">15</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">2</s:key>
<s:key name="tstatsHomePath">volume:_splunk_summaries/$_index_name/datamodel_summary</s:key>
<s:key name="waitPeriodInSecsForManifestWrite">60</s:key>
<s:key name="warmToColdScript"></s:key>
</s:dict>
</content>
</entry>

```

## DELETE

Deletes a definition for a specific {federated\_index\_name}.

### Request parameters

None specific to this method.

### Returned values

None specific to this method.

### Example request and response

Remove the `my_federated_index` stanza from `indexes.conf`.

## 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>
```

# 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/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
<i>disabled</i>	Indicates whether this input is disabled.
<i>index</i>	The index in which to store the gathered data. If no value is present, sends data to the default index.
<i>monitorSubtree</i>	Indicates whether or not to monitor the subtrees of a given Active Directory tree path.
<i>startingNode</i>	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.
<i>targetDc</i>	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
<i>baseline</i>	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.
<i>host</i>	String	Docs-W8R2-Std7	Host name for the Active Directory Monitor.
<i>index</i>	String	default	The index in which to store the gathered data.  If not specified defaults to the default index.
<i>monitorSubtree</i>	Number		<b>Required.</b> Whether or not to monitor the subtree(s) of a given directory tree path. 1 means yes, 0 means no.
<i>name</i>	String		<b>Required.</b> A unique name that represents a configuration or set of configurations for a specific domain controller.
<i>printSchema</i>	Boolean		Indicates whether to print the Active Directory schema. Defaults to true.
<i>source</i>	String		Source for data inputs.
<i>sourcetype</i>	String		Source type of data inputs.

Name	Datatype	Default	Description
<i>startingNode</i>	String		Where in the Active Directory directory tree to start monitoring. If not specified, attempts to start at the root of the directory tree.
<i>targetDc</i>	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
<i>disabled</i>	Indicates whether this input is disabled.
<i>index</i>	The index in which to store the gathered data. If no value is present, send data to the default index.
<i>monitorSubtree</i>	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
<i>baseline</i>	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.
<i>host</i>	String	Docs-W8R2-Std7	Host name for the Active Directory Monitor.
<i>index</i>	String	default	The index in which to store the gathered data.  If not specified defaults to the default index.
<i>monitorSubtree</i> required	Number		Whether or not to monitor the subtree(s) of a given directory tree path. 1 means yes, 0 means no.
<i>printSchema</i>	Boolean		Indicates whether to print the Active Directory schema. Defaults to true.
<i>source</i>	String		Source for data inputs.
<i>sourcetype</i>	String		Source type of data inputs.
<i>startingNode</i>	String		Where in the Active Directory directory tree to start monitoring. If not specified, attempts to start at the root of the directory tree.
<i>targetDc</i>	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
<i>common</i>	Boolean	Indicates whether to return only attributes common to all inputs. The common attributes are as follows. <ul style="list-style-type: none"><li>• app</li><li>• disabled</li><li>• host</li><li>• index</li><li>• owner</li><li>• source</li><li>• sourcetype</li><li>• title</li><li>• updated</li></ul>

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:dict>
  </content>
</entry>

```

```

    <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
<i>common</i>	Boolean	<p>Indicates whether to return only attributes common to all inputs. These common attributes are as follows.</p> <ul style="list-style-type: none"> <li>• app</li> <li>• disabled</li> <li>• host</li> <li>• index</li> <li>• owner</li> <li>• source</li> <li>• sourcetype</li> <li>• title</li> <li>• updated</li> </ul>

### 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: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
------	----------	---------	-------------

<i>dedicatedIoThreads</i>	Number	2	Number of threads used by HTTP Input server.
<i>disabled</i>	Boolean	1	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>enableSSL</i>	Boolean	1	Enable SSL protocol for HTTP data input. 1 = SSL enabled, 0 = SSL disabled.
<i>index</i>	String		Index to store generated events.
<i>indexes</i>	String		Set of indexes allowed for events with this token.
<i>maxSockets</i>	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.
<i>maxThreads</i>	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.
<i>name required</i>	String		Token name ( <i>inputs.conf</i> key)
<i>port</i>	Number	8088	HTTP data input IP port.
<i>source</i>	String		Default source for events with this token.
<i>sourcetype</i>	String		Default sourcetype for events with this token.
<i>useDeploymentServer</i>	Boolean	0 (disabled)	<p>Indicates whether the event collector input writes its configuration to a deployment server repository.</p> <p>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as <code>repositoryLocation</code> in <code>serverclass.conf</code>.</p> <p>Copy the full contents of the <code>splunk_httpinput</code> app directory to this directory for the configuration to work.</p> <p>When enabled, only the tokens defined in the <code>splunk_httpinput</code> app in this repository are viewable and editable on the <b>API and the Data Inputs</b> page in Splunk Web.</p> <p>When disabled, the input writes its configuration to <code>\$SPLUNK_HOME/etc/apps</code> by default.</p> <p>Defaults to 0 (disabled).</p>

### Application-level request parameters

Name	Datatype	Default	Description
<i>disabled</i>	Boolean	1	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>index</i>	String		Index to store generated events.
<i>indexes</i>	String		Set of indexes allowed for events with this token.
<i>name required</i>	String		Token name ( <i>inputs.conf</i> key)
<i>source</i>	String		Default source for events with this token.

Name	Datatype	Default	Description
<i>sourcetype</i>	String		Default sourcetype for events with this token.

## Global returned values

Name	Description		
<i>dedicatedIoThreads</i>	Number of threads used by HTTP Input server.		
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.		
<i>enableSSL</i>	Enable SSL protocol for HTTP data input. 1 = SSL enabled, 0 = SSL disabled.		
<i>host</i>	Host from which the indexer gets data.		
<i>index</i>	Index to store generated events.		
<i>indexes</i>	Set of indexes allowed for events with this token.		
<i>port</i>	HTTP data input IP port.		
<i>_rcvbuf</i>	Socket receive buffer size (bytes).		
<i>source</i>	Default source for events with this token.		
<i>sourcetype</i>	Default sourcetype for events with this token.		
<i>useDeploymentServer</i>	Boolean	0 (disabled)	<p>Indicates whether the event collector input writes its configuration to a deployment server repository.</p> <p>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as <code>repositoryLocation</code> in <code>serverclass.conf</code>.</p> <p>Copy the full contents of the <code>splunk_httpinput</code> app directory to this directory for the configuration to work.</p> <p>When enabled, only the tokens defined in the <code>splunk_httpinput</code> app in this repository are viewable and editable on the <b>API and the Data Inputs</b> page in Splunk Web.</p> <p>When disabled, the input writes its configuration to <code>\$SPLUNK_HOME/etc/apps</code> by default.</p> <p>Defaults to 0 (disabled).</p>

## Application-level returned values

Name	Description
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>source</i>	Source for events with this token.
<i>sourcetype</i>	Sourcetype for events with this token.
<i>token</i>	Token value for sending data to <code>collector/event</code> 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:dict>
  </content>
</entry>
</s:messages>
```

```
<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
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>dedicatedIoThreads</i>	Number of threads for HTTP event collector server.
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>enableSSL</i>	SSL enablement status.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>port</i>	HTTP data event collector IP port.
<i>source</i>	Source for events with this token.
<i>sourcetype</i>	Sourcetype for events with this token.
<i>token</i>	Token value for sending data to <code>collector/event</code> endpoint.
<i>useDeploymentServer</i>	<p>Indicates whether the event collector input writes its configuration to a deployment server repository.</p> <p>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as <code>repositoryLocation</code> in <code>serverclass.conf</code>.</p> <p>Copy the full contents of the <code>splunk_httpinput</code> app directory to this directory for the configuration to work.</p> <p>When enabled, only the tokens defined in the <code>splunk_httpinput</code> app in this repository are viewable and editable on the <b>API and the Data Inputs</b> page in Splunk Web.</p> <p>When disabled, the input writes its configuration to <code>\$SPLUNK_HOME/etc/apps</code> by default.</p> <p>Defaults to 0 (disabled).</p>

### Application-level response data keys



Name	Description
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>source</i>	Source for events with this token.
<i>sourcetype</i>	Sourcetype for events with this token.
<i>token</i>	Token value for sending data to <code>collector/event</code> 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:dict>
  </content>
</entry>
...

```

```

<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
<i>disabled</i>	Boolean	1	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	String		Default host.
<i>index</i>	String		Index to store generated events.
<i>indexes</i>	String		Set of indexes allowed for events with this token.
<i>name</i>	String		<b>Required.</b> Token name ( <i>inputs.conf</i> key)
<i>source</i>	String		Default source for events with this token.
<i>sourcetype</i>	String		Default sourcetype for events with this token.
<i>useDeploymentServer</i>	Boolean	0 (disabled)	<p>Indicates whether the event collector input writes its configuration to a deployment server repository.</p> <p>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as <i>repositoryLocation</i> in <i>serverclass.conf</i>.</p> <p>Copy the full contents of the <i>splunk_httpinput</i> app directory to this directory for the configuration to work.</p> <p>When enabled, only the tokens defined in the <i>splunk_httpinput</i> app in this repository are viewable and editable on the <b>API and the Data Inputs</b> page in Splunk Web.</p> <p>When disabled, the input writes its configuration to <i>\$SPLUNK_HOME/etc/apps</i> by default.</p> <p>Defaults to 0 (disabled).</p>

### Returned values

Name	Description
<i>_rcvbuf</i>	Socket receive buffer size (bytes).

Name	Description
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>source</i>	Source for events with this token.
<i>sourcetype</i>	Sourcetype for events with this token.
<i>token</i>	Token value for sending data to <code>collector/event</code> endpoint.
<i>useDeploymentServer</i>	<p>Indicates whether the event collector input writes its configuration to a deployment server repository.</p> <p>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as <code>repositoryLocation</code> in <code>serverclass.conf</code>.</p> <p>Copy the full contents of the <code>splunk_httpinput</code> app directory to this directory for the configuration to work.</p> <p>When enabled, only the tokens defined in the <code>splunk_httpinput</code> app in this repository are viewable and editable on the <b>API and the Data Inputs</b> page in Splunk Web.</p> <p>When disabled, the input writes its configuration to <code>\$SPLUNK_HOME/etc/apps</code> by default.</p> <p>Defaults to 0 (disabled).</p>

## 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
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.

Name	Description
<i>index</i>	Index to store generated events.
<i>source</i>	Default source for events with this token.
<i>sourcetype</i>	Default sourcetype for events with this token.
<i>token</i>	Token value for sending data to <code>collector/event</code> 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
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>source</i>	Default source for events with this token.
<i>sourcetype</i>	Default sourcetype for events with this token.
<i>token</i>	Token value for sending data to <code>collector/event</code> 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
<i>token</i>	Regenerated token value.

## Example request and response

### XML Request

```
curl -k -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
<i>_TCP_ROUTING</i>	List of TCP forwarding groups, as specified in <code>outputs.conf</code> .
<i>disabled</i>	Indicates if inputs monitoring is disabled.
<i>filecount</i>	Number of files monitored.
<i>host</i>	Name of the Splunk host for which inputs are monitored.
<i>index</i>	The index in which to store the gathered data.
<i>sourcetype</i>	Source type being monitored.  The source type of an event is the format of the data input from which it originates, such as <code>access_combined</code> or <code>cisco_syslog</code> . 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
<i>blacklist</i>	String	Specify a regular expression for a file path. The file path that matches this regular expression is not indexed.
<i>check-index</i>	Boolean	If set to true, the <i>index</i> value is checked to ensure that it is the name of a valid index.
<i>check-path</i>	Boolean	If set to true, the <i>name</i> value is checked to ensure that it exists.
<i>crc-salt</i>	String	A string that modifies the file tracking identity for files in this input. The magic value "<SOURCE>" invokes special behavior (see admin documentation).
<i>disabled</i>	Boolean	Indicates if input monitoring is disabled.
<i>followTail</i>	Boolean	If set to true, files that are seen for the first time is read from the end.
<i>host</i>	String	The value to populate in the host field for events from this data input.
<i>host_regex</i>	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.
<i>host_segment</i>	Number	Use the specified slash-separate segment of the filepath as the host field value.
<i>ignore-older-than</i>	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.
<i>index</i>	String	Which index events from this input should be stored in. Defaults to <code>default</code> .
<i>name</i>	String	<b>Required.</b> The file or directory path to monitor on the system.
<i>recursive</i>	Boolean	Setting this to <code>false</code> prevents monitoring of any subdirectories encountered within this data input.
<i>rename-source</i>	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.
<i>sourcetype</i>	String	The value to populate in the sourcetype field for incoming events.
<i>time-before-close</i>	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.
<i>whitelist</i>	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
<i>disabled</i>	Indicates if inputs monitoring is disabled.
<i>filecount</i>	Number of files being monitored.
<i>host</i>	Name of the Splunk host for which inputs are monitored.
<i>index</i>	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>
  </entry>
</feed>

```

```

<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
<i>blacklist</i>	String	Specify a regular expression for a file path. The file path that matches this regular expression is not indexed.
<i>check-index</i>	Boolean	If set to true, the "index" value is checked to ensure that it is the name of a valid index.
<i>check-path</i>	Boolean	If set to true, the "name" value is checked to ensure that it exists.
<i>crc-salt</i>	String	A string that modifies the file tracking identity for files in this input. The magic value "<SOURCE>" invokes special behavior (see admin documentation).
<i>disabled</i>	Boolean	Indicates if input monitoring is disabled.
<i>followTail</i>	Boolean	If set to true, files that are seen for the first time is read from the end.
<i>host</i>	String	The value to populate in the host field for events from this data input.
<i>host_regex</i>	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.
<i>host_segment</i>	Number	Use the specified slash-separate segment of the filepath as the host field value.
<i>ignore-older-than</i>	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.
<i>index</i>	String	Which index events from this input should be stored in. Defaults to <code>default</code> .
<i>recursive</i>	Boolean	Setting this to "false" prevents monitoring of any subdirectories encountered within this data input.
<i>rename-source</i>	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.
<i>sourcetype</i>	String	The value to populate in the sourcetype field for incoming events.
<i>time-before-close</i>	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.
<i>whitelist</i>	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
<i>Bytes Indexed</i>	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.
<i>Offset</i>	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.
<i>Size</i>	Size of the source file, in bytes.  You can obtain the percentage of a source file read by calculating offset/size.
<i>Sources Indexed</i>	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.
<i>Spool Time</i>	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
<i>host</i>	String		The value of the <code>host</code> field to be applied to data from this file.
<i>host_regex</i>	String		A regex to be used to extract a <code>host</code> field from the path.  If the path matches this regular expression, the captured value is used to populate the <code>host</code> field for events from this data input. The regular expression must have one capture group.
<i>host_segment</i>	Number		Use the specified slash-separate segment of the path as the <code>host</code> field value.
<i>index</i>	String		The destination index for data processed from this file.
<i>name</i>	String		<b>Required.</b> The path to the file to be indexed. The file must be locally accessible by the server.
<i>rename-source</i>	String		The value of the <code>source</code> field to be applied to data from this file.
<i>sourcetype</i>	String		The value of the <code>sourcetype</code> 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
<i>Bytes Indexed</i>	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.
<i>Offset</i>	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.
<i>Size</i>	Size of the source file, in bytes.  You can obtain the percentage of a source file read by calculating offset/size.
<i>Sources Indexed</i>	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.
<i>Spool Time</i>	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
<i>baseline</i>	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.
<i>disabled</i>	Indicats whether this input is disabled.
<i>hive</i>	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.
<i>index</i>	Specifies the index that this input should send the data to.  If no value is present, defaults to the default index.
<i>monitorSubnodes</i>	Indicates whether to monitor all Registry hives beneath the specified hive.
<i>proc</i>	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.
<i>type</i>	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
<i>baseline</i>	Boolean		<b>Required.</b> Indicate whether to establish a baseline value for the registry keys. Use 1 to establish the baseline, 0 for no baseline.
<i>hive</i>	String		<b>Required.</b> Specify the registry hive for monitoring changes.
<i>name</i>	String		<b>Required.</b> Name of the configuration stanza.
<i>proc</i>	String		<b>Required.</b> Specify a regex for collecting changes if a process name matches the regex.
<i>type</i>	String		<b>Required.</b> List registry event types that you want to monitor. Separate each type with a pipe (' ') character. For example, set   create   delete   rename
<i>disabled</i>	Boolean		Indicates whether the monitoring is disabled.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>monitorSubnodes</i>	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
<i>baseline</i>	Indicates whether to get a baseline of Registry events when Splunk software starts.
<i>disabled</i>	Indicates if the input is disabled.
<i>hive</i>	<p>Regular expression for Registry hives that this input should monitor for Registry access.</p> <p>Matches against the Registry key which was accessed.</p> <p>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.</p>
<i>index</i>	<p>Specifies the index that this input should send the data to.</p> <p>If no value is present, defaults to the default index.</p>
<i>monitorSubnodes</i>	Indicates whether to monitor all Registry hives beneath the specified hive.
<i>proc</i>	<p>Regular expression for processes this input should monitor for Registry access.</p> <p>It matches against the process name which performed the Registry access.</p> <p>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.</p>
<i>type</i>	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
<i>baseline</i>	Number		<b>Required.</b> Specifies whether or not to establish a baseline value for the registry keys. 1 means yes, 0 no.
<i>hive</i>	String		<b>Required.</b> Specifies the registry hive under which to monitor for changes.
<i>proc</i>	String		<b>Required.</b> Specifies a regex. If specified, collect changes if a process name matches that regex.
<i>type</i>	String		<b>Required.</b> A list of registry events types that you want to monitor. Separate each type with a pipe (' ') character.  For example:  set   create   delete   rename
<i>disabled</i>	Number		Indicates whether the monitoring is disabled.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>monitorSubnodes</i>	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
<i>disabled</i>	Specifies whether the input script is disabled.
<i>endtime</i>	If available, the time when the script stopped executing.
<i>group</i>	The name of the inputstatus group, which is always "exec commands."
<i>host</i>	Host with which these data are identified.
<i>index</i>	Sets the index for events from this input. Defaults to the main index.
<i>interval</i>	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.
<i>source</i>	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::'.
<i>sourcetype</i>	

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.
<i>starttime</i>	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>
```

```

    </content>
  </entry>
</feed>

```

### POST

Configure scripted input settings.

### Request parameters

Name	Datatype	Default	Description
<i>disabled</i>	Boolean		Specifies whether the input script is disabled.
<i>host</i>	String		Sets the host for events from this input. Defaults to whatever host sent the event.
<i>index</i>	String	default	Sets the index for events from this input. Defaults to the main index.
<i>interval</i>	Number	60.0	<b>Required.</b> 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.
<i>name</i>	String		<b>Required.</b> Specify the name of the scripted input.
<i>passAuth</i>	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.
<i>rename-source</i>	String		Specify a new name for the source field for the script.
<i>source</i>	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::'.  <b>Note:</b> 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.
<i>sourcetype</i>	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
<i>script</i>	String		<b>Required.</b> 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
<i>disabled</i>	Specifies whether the input script is disabled.
<i>group</i>	The name of the inputstatus group, which is always "exec commands."
<i>host</i>	Host these data are identified with.
<i>index</i>	Sets the index for events from this input. Defaults to the main index.
<i>interval</i>	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:dict>
    </content>
  </entry>
</feed>

```

```

    <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
<i>disabled</i>	Boolean		Specifies whether the input script is disabled.
<i>host</i>	String		Sets the host for events from this input. Defaults to whatever host sent the event.
<i>index</i>	String	default	Sets the index for events from this input. Defaults to the main index.
<i>interval</i>	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.
<i>passAuth</i>	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.
<i>rename-source</i>	String		Specify a new name for the source field for the script.
<i>source</i>	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::'.  <b>Note:</b> 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.
<i>sourcetype</i>	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
<i>_rcvbuf</i>	[Deprecated]
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>group</i>	Set to <code>listenerports</code> for listening ports.
<i>host</i>	The default value to fill in for events lacking a host value.
<i>index</i>	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"/>
  </entry>
</feed>
```

```

<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
<i>SSL</i>	Boolean		If SSL is not already configured, error is returned
<i>connection_host</i>	Enum	dns	<p>Valid values: (ip   dns   none)</p> <p>Set the host for the remote server that is sending data.</p> <p><i>ip</i> sets the host to the IP address of the remote server sending data.</p> <p><i>dns</i> sets the host to the reverse DNS entry for the IP address of the remote server sending data.</p> <p><i>none</i> leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</p> <p>Default value is <i>dns</i>.</p>
<i>disabled</i>	Boolean		Indicates whether the input is disabled.
<i>host</i>	String		The default value to fill in for events lacking a host value.
<i>name</i>	Number		<b>Required.</b> The port number of this input.
<i>queue</i>	"parsingQueue"   "indexQueue"	"parsingQueue"	Specifies where the input processor should deposit the events it reads.
<i>restrictToHost</i>	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
<i>_rcvbuf</i>	[Deprecated]
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>group</i>	Set to <code>listenerports</code> for listening ports.
<i>host</i>	The default value to fill in for events lacking a host value.
<i>index</i>	The index in which to store generated events.
<i>restrictToHost</i>	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>
```



```

    </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
<i>connection</i>	Identifies the connection to port.
<i>servername</i>	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
<i>_rcvbuf</i>	[Deprecated]
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>group</i>	Set to <code>listenerports</code> for listening ports.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	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
<i>connection_host</i>	Enum	dns	<p>Valid values: (ip   dns   none)</p> <p>Set the host for the remote server that is sending data.</p> <p><i>ip</i> sets the host to the IP address of the remote server sending data.</p> <p><i>dns</i> sets the host to the reverse DNS entry for the IP address of the remote server sending data.</p> <p><i>none</i> leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</p> <p>Default value is <i>ip</i>.</p>
<i>disabled</i>	Boolean		Indicates whether the inputs are disabled.
<i>host</i>	String		Host from which the indexer gets data.
<i>index</i>	String	default	Index to store generated events.
<i>name required</i>	String		The input port which receives raw data.
<i>queue</i>	Enum		<p>Valid values: (parsingQueue   indexQueue)</p> <p>Specifies where the input processor should deposit the events it reads. Defaults to parsingQueue.</p> <p>Set queue to <i>parsingQueue</i> 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 <i>props.conf</i> and the online documentation at "Monitor files and directories with inputs.conf"</p> <p>Set queue to <i>indexQueue</i> to send your data directly into the index.</p>

Name	Datatype	Default	Description
<i>rawTcpDoneTimeout</i>	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 <i>name</i> remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is completely received.
<i>restrictToHost</i>	String		Allows for restricting this input to only accept data from the host specified here.
<i>SSL</i>	Boolean		
<i>source</i>	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::'.  <i>Note:</i> 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.
<i>sourcetype</i>	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"/>
</feed>
```

```
... 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
<i>_rcvbuf</i>	[Deprecated]
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>group</i>	Set to <code>listenerports</code> for listening ports.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>restrictToHost</i>	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
			<p>Set the host for the remote server that is sending data.</p> <p><code>ip</code> sets the host to the IP address of the remote server sending data.</p> <p><code>dns</code> sets the host to the reverse DNS entry for the IP address of the remote server sending data.</p> <p><code>none</code> leaves the host as specified in <code>inputs.conf</code>, which is typically the Splunk system hostname.</p> <p>Default value is <code>ip</code>.</p>
<code>disabled</code>	Boolean		Indicates whether the inputs are disabled.
<code>host</code>	String		Host from which the indexer gets data.
<code>index</code>	String	default	Index to store generated events.
<code>queue</code>	Enum		<p>Valid values: (<code>parsingQueue</code>   <code>indexQueue</code>)</p> <p>Specifies where the input processor should deposit the events it reads. Defaults to <code>parsingQueue</code>.</p> <p>Set <code>queue</code> to <code>parsingQueue</code> to apply <code>props.conf</code> and other parsing rules to your data. For more information about <code>props.conf</code> and rules for timestamping and linebreaking, refer to <code>props.conf</code> and Monitor files and directories with <code>inputs.conf</code>.</p> <p>Set <code>queue</code> to <code>indexQueue</code> to send your data directly into the index.</p>
<code>rawTcpDoneTimeout</code>	Number		<p>Specifies in seconds the timeout value for adding a Done-key. Default value is 10 seconds.</p> <p>If a connection over the port specified by <code>name</code> remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is completely received.</p>
<code>restrictToHost</code>	String		Allows for restricting this input to only accept data from the host specified here.
<code>source</code>	String		<p>Sets the source key/field for events from this input. Defaults to the input file path.</p> <p>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::'.</p> <p><i>Note:</i> 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.</p>
<code>sourcetype</code>	String		<p>Set the source type for events from this input.</p> <p>"sourcetype=" is automatically prepended to <code>&lt;string&gt;</code>.</p>

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
<i>connection</i>	IP address and port of the source connecting to this TCP input port.
<i>servername</i>	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/splunkcptoken

https://<host>:<mPort>/services/data/inputs/tcp/splunkcptoken  
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/splunkcptoken/{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/splunkcptoken

XML Response

<title>splunkcptoken</title>  
  <id>https://localhost:8089/services/data/inputs/tcp/splunkcptoken</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:dict>
  </content>
</entry>
</s:messages>
</s:messages>

```

```

        </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:dict>
    </content>
</entry>

```

```

    <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
<i>name</i>	String	None	Required. Name for the token to create.
<i>token</i>	String	None	Optional. Token value to use. If unspecified, a token is generated automatically.

### Returned values

Name	Description
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>token</i>	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:dict>
          <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>

```

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

---

## data/inputs/tcp/splunkcptoken/{name}

`https://<host>:<mPort>/services/data/inputs/tcp/splunkcptoken/{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
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>token</i>	Token value.

### Example request and response

### XML Request

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/splunkcptoken
```

### XML Response

```
...
<title>splunkcptoken</title>
<id>https://localhost:8089/services/data/inputs/tcp/splunkcptoken</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/splunkcptoken/_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
<i>token</i>	String	None	New token value.

Pagination and filtering parameters can be used with this method.

### Returned values

Name	Description
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>token</i>	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
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	Index to store generated events.
<i>token</i>	Token value.

### Example request and response

### XML Request

```
curl -k -X "DELETE" -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunkcptoken/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>splunkcptoken</title>
  <id>https://localhost:8089/services/data/inputs/tcp/splunkcptoken</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
<i>_rcvbuf</i>	[Deprecated]
<i>cipherSuite</i>	Specifies list of acceptable ciphers to use in ssl.
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	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
<i>_rcvbuf</i>	[Deprecated]
<i>cipherSuite</i>	Specifies list of acceptable ciphers to use in ssl.
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	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
<i>disabled</i>	Boolean		Indicates whether the inputs are disabled.
<i>password</i>	String		Server certificate password, if any.
<i>requireClientCert</i>	Boolean		Determines whether a client must authenticate.
<i>rootCA</i>	String		Certificate authority list (root file)
<i>serverCert</i>	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
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>group</i>	Set to <code>listenerports</code> for listening ports.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	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
<i>connection_host</i>	Enum	ip	<p>Valid values: (ip   dns   none)</p> <p>Set the host for the remote server that is sending data.</p> <p><i>ip</i> sets the host to the IP address of the remote server sending data.</p> <p><i>dns</i> sets the host to the reverse DNS entry for the IP address of the remote server sending data.</p> <p><i>none</i> leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</p> <p>Default value is <i>ip</i>.</p>
<i>disabled</i>	Boolean		Indicates if the input is disabled.
<i>host</i>	String		<p>The value to populate in the host field for incoming events.</p> <p>This is used during parsing/indexing, in particular to set the host field. It is also the host field used at search time.</p>
<i>index</i>	String	default	Which index events from this input should be stored in.

Name	Datatype	Default	Description
<i>name</i>	String		<b>Required.</b> The UDP port that this input should listen on.
<i>no_appending_timestamp</i>	Boolean		If set to true, prevents Splunk software from prepending a timestamp and hostname to incoming events.
<i>no_priority_stripping</i>	Boolean		If set to true, Splunk software does not remove the priority field from incoming syslog events.
<i>queue</i>	String		Which queue events from this input should be sent to. Generally this does not need to be changed.
<i>restrictToHost</i>	String		Restrict incoming connections on this port to the host specified here.  If this is not set, the value specified in <code>[udp://&lt;remote server&gt;:&lt;port&gt;]</code> in <code>inputs.conf</code> is used.
<i>source</i>	String		The value to populate in the source field for incoming events. The same source should not be used for multiple data inputs.
<i>sourcetype</i>	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
<i>_rcvbuf</i>	Socket receive buffer size (bytes).
<i>disabled</i>	Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.
<i>group</i>	Set to <code>listenerports</code> for listening ports.
<i>host</i>	Host from which the indexer gets data.
<i>index</i>	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:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</feed>
```

```

        <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
<i>connection_host</i>	Enum	ip	<p>Valid values: (ip   dns   none)</p> <p>Set the host for the remote server that is sending data.</p> <p><b>ip</b> sets the host to the IP address of the remote server sending data.</p> <p><b>dns</b> sets the host to the reverse DNS entry for the IP address of the remote server sending data.</p> <p><b>none</b> leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</p> <p>Default value is <b>ip</b>.</p>
<i>disabled</i>	Boolean		Indicates if the input is disabled.
<i>host</i>	String		<p>The value to populate in the host field for incoming events.</p> <p>This is used during parsing/indexing, in particular to set the host field. It is also the host field used at search time.</p>
<i>index</i>	String	default	Which index events from this input should be stored in.



Name	Datatype	Default	Description
<i>no_appending_timestamp</i>	Boolean		If set to true, prevents Splunk software from prepending a timestamp and hostname to incoming events.
<i>no_priority_stripping</i>	Boolean		If set to true, Splunk software does not remove the priority field from incoming syslog events.
<i>queue</i>	String		Which queue events from this input should be sent to. Generally this does not need to be changed.
<i>restrictToHost</i>	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.
<i>source</i>	String		The value to populate in the source field for incoming events. The same source should not be used for multiple data inputs.
<i>sourcetype</i>	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
<i>disabled</i>	Indicates whether the inputs are disabled.
<i>group</i>	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"/>
  </entry>
</feed>
```

```

<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
<i>lookup_host</i>	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
<i>disabled</i>	Indicates if the input is disabled.
<i>hosts</i>	Hosts you are monitoring.
<i>index</i>	Index to store data. If not specified defaults to the default index.
<i>logs</i>	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
<i>hosts</i>	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.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>logs</i>	String		List of event log names from which to gather data: <ul style="list-style-type: none"><li>• WMI collection format (CSV) example: logs=Application%2CSystem%2CSetup%2CSecurity</li><li>• Native event log collection format example: logs=Application&amp;logs=System&amp;logs=Setup</li></ul>
<i>lookup_host</i>	String		<b>Required.</b> Host from which to monitor log events. To specify additional hosts to be monitored using WMI, use the "hosts" parameter.
<i>name</i>	String		<b>Required.</b> 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
<i>disabled</i>	Indicates if the input is disabled.
<i>hosts</i>	Monitored hosts.
<i>index</i>	Index to store data.
<i>logs</i>	List of event log channels to monitor.
<i>lookup_host</i>	Host from which to monitor log events.
<i>name</i>	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
<i>disabled</i>	Indicates if the input is disabled.
<i>hosts</i>	Monitored hosts.
<i>index</i>	Index to store data. If not specified defaults to the default index.
<i>logs</i>	List of event log channels to monitor.
<i>lookup_host</i>	Host from which to monitor log events.
<i>name</i>	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
<i>hosts</i>	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.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>logs</i>	String		A comma-separated list of event log names to gather data from.
<i>lookup_host</i>	String		<b>Required.</b> 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
<i>disabled</i>	Indicates if the input is disabled.
<i>hosts</i>	Monitored hosts.
<i>index</i>	Index to store data.
<i>logs</i>	List of event log channels to monitor.
<i>lookup_host</i>	Host from which to monitor log events.
<i>name</i>	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
<i>class</i>	The WMI performance object class being monitored.
<i>disabled</i>	Indicates whther the input is disbled.
<i>fields</i>	The WMI performance counters being monitored.
<i>index</i>	The index to which you are sending input data.
<i>instances</i>	Instances of the WMI performance counter.

Name	Description
<i>interval</i>	The interval, in seconds, at which the WMI provider(s) are queried.
<i>name</i>	the name of the input.
<i>server</i>	The server you are monitoring.
<i>wql</i>	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:dict>
    </content>
  </entry>
</feed>
```

```

        </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
<i>classes</i>	String		<b>Required.</b> A valid WMI class name.
<i>disabled</i>	Number	0	Disables the given collection.
<i>fields</i>	String	1. *	Properties (fields) that you want to gather from the given class. Specify each property as a separate argument to the POST operation.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>instances</i>	String	empty	Instances of a given class for which data is gathered. Specify each instance as a separate argument to the POST operation.
<i>interval</i>	Number		<b>Required.</b> The interval, in seconds, at which the WMI provider(s) is queried.
<i>lookup_host</i>	String		<b>Required.</b> 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.
<i>name</i>	String		<b>Required.</b> 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.
<i>server</i>	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 <i>lookup_host</i> .

### Returned values

Name	Description
<i>classes</i>	A valid WMI class name.
<i>disabled</i>	Indicates if the input is disabled.
<i>fields</i>	Properties (fields) that you want to gather from the given class.

Name	Description
<i>index</i>	The index in which to store the gathered data.
<i>instances</i>	Instances of a given class for which data is gathered.
<i>interval</i>	The interval, in seconds, at which the WMI provider(s) is queried.
<i>lookup_host</i>	Host from which to monitor log events.
<i>server</i>	Servers from which to gather data. Used if you need to gather from more than a single machine. See also <i>lookup_host</i> .
<i>wql</i>	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
<i>classes</i>	A valid WMI class name.
<i>disabled</i>	Indicates if the input is disabled.
<i>fields</i>	Properties (fields) that you want to gather from the given class.
<i>index</i>	The index in which to store the gathered data.
<i>instances</i>	Instances of a given class for which data is gathered.
<i>interval</i>	The interval, in seconds, at which the WMI provider(s) is queried.
<i>lookup_host</i>	Host from which to monitor log events.
<i>name</i>	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.
<i>server</i>	Servers from which to gather data from. Used if you need to gather from more than a single machine. See also lookup_host.
<i>wql</i>	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:dict>
  </content>
</entry>
</s:messages>
</rest>

```

```

    <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
<i>classes</i>	String		<b>Required.</b> A valid WMI class name.
<i>disabled</i>	Number		Disables the given collection.
<i>fields</i>	String		Properties (fields) that you want to gather from the given class. Specify each property as a separate argument to the POST operation.
<i>index</i>	String		The index in which to store the gathered data.
<i>instances</i>	String		Instances of a given class for which data is gathered. Specify each instance as a separate argument to the POST operation.
<i>interval</i>	Number		<b>Required.</b> The interval, in seconds, at which the WMI provider(s) is queried.
<i>lookup_host</i>	String		<b>Required.</b> 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.
<i>server</i>	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
<i>classes</i>	A valid WMI class name.
<i>disabled</i>	Indicates if the input is disabled.
<i>fields</i>	Properties (fields) that you want to gather from the given class.
<i>index</i>	The index in which to store the gathered data.
<i>instances</i>	Instances of a given class for which data is gathered.
<i>interval</i>	The interval, in seconds, at which the WMI provider(s) are queried.
<i>lookup_host</i>	Host from which to monitor log events.

Name	Description
<i>name</i>	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.
<i>server</i>	Servers from which to gather data. Used if you need to gather from more than a single machine. See also lookup_host.
<i>wql</i>	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
<i>counters</i>	List of valid Performance Monitor counters.
<i>disabled</i>	Indicates whether the input is disabled.
<i>index</i>	The index that this input should send data to. If no value is present, send data to the default index.
<i>instances</i>	List of valid instances for a Performance Monitor counter.
<i>interval</i>	How often, in seconds, to poll for new data.
<i>object</i>	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
<i>counters</i>	String		A set of counters to monitor. A '*' is equivalent to all counters.  Specify each counter as a separate argument to the POST operation.
<i>host</i>	String	Docs-W8R2-Std7	Name of the host for the Windows Performance Monitor.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>instances</i>	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.
<i>interval</i>	Number		How frequently, in seconds, to poll for new data.
<i>name</i> 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.
<i>object</i>	String		A valid performance monitor object (for example, 'Process,' 'Server,' 'PhysicalDisk.')
<i>source</i>	String		Source for inputs.
<i>sourcetype</i>	String		Source type of input.

## Returned values

Name	Description
<i>counters</i>	List of valid Performance Monitor counters.
<i>disabled</i>	Indicates whether the input is disabled.
<i>host</i>	Name of the host for the Windows Performance Monitor.
<i>index</i>	The index that this input should send data to.  If no value is present, send data to the default index.
<i>instances</i>	List of valid instances for a Performance Monitor counter.
<i>interval</i>	How frequently, in seconds, to poll for new data.
<i>object</i>	A valid Performance Monitor object as defined within Performance Monitor.
<i>source</i>	Source for inputs.
<i>sourcetype</i>	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
<i>counters</i>	List of valid Performance Monitor counters.
<i>disabled</i>	Indicates whether the input is disabled.
<i>index</i>	The index that this input should send data to.  If no value is present, send data to the default index.
<i>instances</i>	List of valid instances for a Performance Monitor counter.
<i>interval</i>	How often, in seconds, to poll for new data.
<i>object</i>	A valid Performance Monitor object as defined within Performance Monitor.



Name	Description

## 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
<i>counters</i>	String		A set of counters to monitor. A '*' is equivalent to all counters.  Specify each counter as a separate argument to the POST operation.
<i>host</i>	String	Docs-W8R2-Std7	Name of the host for the Windows Performance Monitor.
<i>index</i>	String	default	The index in which to store the gathered data.
<i>instances</i>	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.
<i>interval</i>	Number		How frequently, in seconds, to poll for new data.
<i>object</i>	String		A valid performance monitor object (for example, 'Process,' 'Server,' 'PhysicalDisk.')
<i>source</i>	String		Source for inputs.
<i>sourcetype</i>	String		Source type of input.

### Returned values

Name	Description
<i>counters</i>	List of valid Performance Monitor counters.
<i>disabled</i>	Indicates whether the input is disabled.
<i>host</i>	Name of the host for the Windows Performance Monitor.

Name	Description
<i>index</i>	The index that this input should send data to. If no value is present, send data to the default index.
<i>instances</i>	List of valid instances for a Performance Monitor counter.
<i>interval</i>	How frequently, in seconds, to poll for new data.
<i>object</i>	A valid Performance Monitor object as defined within Performance Monitor,
<i>source</i>	Source for inputs.
<i>sourcetype</i>	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
<i>description</i>	Provides descriptive text for title shown on the <b>Data inputs</b> manager page. The description also appears on the <b>Add new data inputs</b> page.
<i>endpoint</i>	Contains one or more <arg> elements, which define the parameters to an endpoint.
<i>streaming_mode</i>	Indicates the streaming mode for the modular input. Valid values are <code>xml</code> and <code>simple</code> .
<i>title</i>	The label for a modular input script. The title appears on the <b>Data inputs</b> 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:dict>
  </content>
</entry>

```

```

        </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
<i>description</i>	<p>The label for a modular input script.</p> <p>The label appears in the <b>Data inputs</b> manager page.</p>
<i>endpoint</i>	Contains one or more <arg> elements, which define the parameters to an endpoint.
<i>streaming_mode</i>	<p>Indicates the streaming mode for the modular input. Valid values are <code>xml</code> or <code>simple</code> (plain text).</p> <p>Contains one or more &lt;arg&gt; elements, which define the parameters to an endpoint.</p>
<i>title</i>	The label for a modular input script. The label appears in the <b>Data inputs</b> 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:dict>
  </content>
</entry>

```

```
</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
<i>input.path</i>	String		<b>Required.</b> The absolute file path to a local file that you want to preview data returned from indexing.
<i>props.&lt;props_attr&gt;</i>	String		Define a new sourcetype in <code>props.conf</code> 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
------	----------	---------	-------------

Name	Datatype	Default	Description
<arbitrary_data>	String		<b>Required.</b> 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
<code>&lt;data_stream&gt;</code>	String		<b>Required.</b> Raw event text. This does not need to be presented as a complete HTTP request, but can be streamed in as data is available.
<code>host</code>	String		The value to populate in the host field for events from this data input.
<code>host_regex</code>	String		A regular expression used to extract the host value from each event.
<code>index</code>	String		The index to send events from this input to.
<code>source</code>	String		The source value to fill in the metadata for this input's events.
<code>sourcetype</code>	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 67bed982celaf9ba2e393b15ed63c916")
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
<i>busiest_thread_name</i>	The name of the busiest pipeline thread within the pipeline set for past calculation period.
<i>dutycycle_ratio</i>	The dutycycle ratio of the busiest pipeline thread within the pipeline set for past calculation period.
<i>requests_last_period</i>	The number of ingestion requests processed by the pipeline set in the past calculation period.
<i>share</i>	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="duty_cycle_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
<i>channel</i>	See description	Required if <code>useAck</code> is enabled. Pass in the channel GUID as a string parameter or using the <code>"x-splunk-request-channel"</code> header.
<i>event</i>	string	Required. Event payload key-value. Value can be a string or a JSON object.  JSON example: <code>{"event": {"message": "Access log test message"}}</code> String example: <code>"event": "Access log test message."</code>
<i>fields</i>	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 <code>"severity"</code> field gets the value <code>"INFO"</code> and the <code>"category"</code> key gets both <code>"foo"</code> and <code>"bar"</code> values. <code>-d {"event": "something happened", "fields": {"severity": "INFO", "category": ["foo", "bar"]}}</code>
<i>host</i>	string	Host name. Specify with the <i>host</i> query string parameter. Sets a default for all events in the request. The default host name can be overridden.
<i>index</i>	string	Index name. Specify with the <i>index</i> query string parameter. Sets a default for all events in the request. The default index name can be overridden.
<i>source</i>	string	User-defined event source. Specify with the <i>source</i> query string parameter. Sets a default for all events in the request. The default source can be overridden.
<i>sourcetype</i>	string	User-defined event sourcetype. Specify with the <i>sourcetype</i> query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.
<i>time</i>	string or unsigned integer	Epoch-formatted time. Specify with the <i>time</i> query string parameter. Sets a default for all events in the request. The default time can be overridden.

## Returned values

Name	Description
<i>text</i>	Human readable status, same value as <i>code</i> .
<i>code</i>	Machine format status, same value as <i>text</i> .
<i>invalid-event-number</i>	When errors occur, indicates the zero-based index of first invalid event in an event sequence.
<i>ackId</i>	If <code>useACK</code> is enabled for the token, indicates the <code>ackId</code> 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

Status Code	HTTP status code ID	HTTP status code	Status message
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 -k 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
-k 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
<i>channel</i>	See description	Required. Pass in the channel GUID as the <i>channel</i> string parameter or using the <code>x-splunk-request-channel</code> header.
"acks"	JSON object	Required. JSON object with an array of ack ID values. Include in the request payload.

## Returned values

Name	Description
<i>acks</i>	<p>Contains the key/value pairs for each ACK ID requested. For each key in the "acks" object, a <code>true</code> value means the ACK ID's events were indexed. A <code>false</code> value means that indexing status is unknown. For example, an event may have an indexing delay long enough that it is no longer tracked.</p> <p>Here is an example response.</p> <pre>{"acks" : { "0" : true, "1" : false, "2" : true, "3" : false}}</pre>

## 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 -k 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.

## 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. HEC health is determined if there is space available in the queue.

This endpoint works identically to `services/health/1.0`, except `services/health/1.0` introduces a format version for future scalability. For more information, see `services/collector/health/1.0`.

### 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

## 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

Status Code	Description
400	Invalid HEC token
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
<i>host</i>	String	Host name. Specify with the <i>host</i> query string parameter. Sets a default for all events in the request. Can be overridden.
<i>index</i>	String	Index name. Specify with the <i>index</i> query string parameter. Sets a default for all events in the request. Can be overridden.
<i>source</i>	String	User-defined event source. Specify with the <i>source</i> query string parameter. Sets a default for all events in the request. The default source can be overridden.
<i>sourcetype</i>	string	User-defined event sourcetype. Specify with the <i>sourcetype</i> query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.
<i>time</i>	string or unsigned integer	Epoch-formatted time. Specify with the <i>time</i> 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 -k 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
<i>channel</i>	See description.	<b>Required.</b> Pass in the channel GUID as the <i>channel</i> string parameter or using the <code>x-splunk-request-channel</code> header.
<i>host</i>	String	Host name. Specify with the <i>host</i> query string parameter. Sets a default for all events in the request. Can be overridden.
<i>index</i>	String	Index name. Specify with the <i>index</i> query string parameter. Sets a default for all events in the request. Can be overridden.
<i>source</i>	String	User-defined event source. Specify with the <i>source</i> query string parameter. Sets a default for all events in the request. The default source can be overridden.
<i>sourcetype</i>	string	User-defined event sourcetype. Specify with the <i>sourcetype</i> query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.
<i>time</i>	string or unsigned integer	Epoch-formatted time. Specify with the <i>time</i> 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 -k -X POST 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 -k -X POST 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 -k -X POST 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
-k 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 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/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
<i>max_size</i>	Maximum <i>name</i> volume size limit (MB):  <i>infinite</i> = No maximum specified.
<i>name</i>	Volume name
<i>total_size</i>	Total <i>name</i> volume capacity (MB). If <i>max_size</i> is <i>infinite</i> , 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
<i>max_size</i>	Maximum <i>name</i> volume size limit (MB).

Name	Description
	<code>infinite</code> = No maximum specified (i.e., 0, the default)
<code>name</code>	Volume name.
<code>total_size</code>	Total <code>name</code> volume capacity (MB). If <code>max_size</code> is <code>infinite</code> , 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
<i>datatype</i>	String	event	Valid values: (all   event   metric). Specifies the type of index.

### Returned values

Name	Description
<i>assureUTF8</i>	Indicates whether all data retrieved from the index is proper UTF8. If enabled (set to True), degrades indexing performance.  This is a global setting, not a per index setting.
<i>blockSignSize</i>	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.
<i>blockSignatureDatabase</i>	The index that stores block signatures of events.  This is a global setting, not a per index setting.
<i>coldPath</i>	Filepath to the cold databases for the index.
<i>coldPath_expanded</i>	Absolute filepath to the cold databases.
<i>coldToFrozenDir</i>	Destination path for the frozen archive. Used as an alternative to a <code>coldToFrozenScript</code> . Splunk software automatically puts frozen buckets in this directory.  Bucket freezing policy is as follows: <ul style="list-style-type: none"><li>• New style buckets (4.2 and on): removes all files but the rawdata  To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</li><li>• Old style buckets (Pre-4.2): gzip all the <code>.data</code> and <code>.tsidx</code> files  To thaw, unzip the zipped files and move the bucket into the thawed directory</li></ul>

Name	Description
	If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.
<i>coldToFrozenScript</i>	Path to the archiving script.  See the POST parameter description for details.
<i>compressRawdata</i>	This value is ignored. splunkd process always compresses raw data.
<i>currentDBSizeMB</i>	Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.
<i>datatype</i>	The type of index (event   metric).
<i>defaultDatabase</i>	If no index destination information is available in the input data, the index shown here is the destination of such data.
<i>disabled</i>	Indicates if the index is disabled.
<i>enableRealtimeSearch</i>	Indicates if this is a real-time search.  This is a global setting, not a per index setting.
<i>frozenTimePeriodInSecs</i>	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.
<i>homePath</i>	An absolute path that contains the hot and warm buckets for the index.
<i>homePath_expanded</i>	An absolute filepath to the hot and warm buckets for the index.
<i>indexThreads</i>	Number of threads used for indexing.  This is a global setting, not a per index setting.
<i>isInternal</i>	Indicates if this is an internal index (for example, _internal, _audit).
<i>isReady</i>	Indicates if the index is properly initialized.
<i>lastInitTime</i>	Last time the index processor was successfully initialized.  This is a global setting, not a per index setting.
<i>maxConcurrentOptimizes</i>	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.
<i>maxDataSize</i>	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. <ul style="list-style-type: none"> <li>• "auto" sets the size to 750MB.</li> <li>• "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</li> </ul> <p>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.</p>

Name	Description
	<p>If you specify an invalid number or string, <code>maxDataSize</code> is auto-tuned.</p> <p><i>Note:</i> The precise size of your warm buckets may vary from <code>maxDataSize</code>, due to post-processing and timing issues with the rolling policy.</p>
<code>maxHotBuckets</code>	<p>Maximum hot buckets that can exist per index. Defaults to 3.</p> <p>When <code>maxHotBuckets</code> 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 <code>maxHotIdleSecs</code>, which can also cause hot buckets to roll.</p>
<code>maxHotIdleSecs</code>	<p>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).</p> <p>If a hot bucket exceeds <code>maxHotIdleSecs</code>, Splunk software rolls it to warm. This setting operates independently of <code>maxHotBuckets</code>, which can also cause hot buckets to roll.</p>
<code>maxHotSpanSecs</code>	<p>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).</p> <p><i>Note:</i> 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.</p>
<code>maxMemMB</code>	<p>The amount of memory, in MB, allocated for indexing.</p> <p>This is a global setting, not a per index setting.</p>
<code>maxMetaEntries</code>	<p>Sets the maximum number of unique lines in <code>.data</code> files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).</p> <p>If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to <code>Strings.data</code> hitting this limit, the culprit may be the <code>punct</code> field in your data. If you do not use <code>punct</code>, it may be best to simply disable this (see <code>props.conf.spec</code> in <code>\$SPLUNK_HOME/etc/system/README</code>).</p> <p>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.</p>
<code>maxRunningProcessGroups</code>	<p>Maximum number of processes that the indexer fires off at a time.</p> <p>This is a global setting, not a per index setting.</p>
<code>maxTime</code>	ISO8601 timestamp of the newest event time in the index.
<code>maxTotalDataSizeMB</code>	The maximum size of an index, in MB.
<code>maxWarmDBCount</code>	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.
<code>memPoolMB</code>	<p>Determines how much memory is given to the indexer memory pool.</p> <p>This is a global setting, not a per-index setting.</p>



Name	Description
<i>minRawFileSyncSecs</i>	<p>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</p> <p>The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices.</p> <p>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.</p> <p>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.</p>
<i>minTime</i>	ISO8601 timestamp of the oldest event time in the index.
<i>partialServiceMetaPeriod</i>	<p>Related to serviceMetaPeriod. By default it is turned off (zero).</p> <p>If set, it enables metadata sync every &lt;integer&gt; 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.</p> <p>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.</p> <p>If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</p>
<i>quarantineFutureSecs</i>	<p>Events with timestamp of <code>quarantineFutureSecs</code> newer than "now" that are dropped into quarantine bucket. Defaults to 2592000 (30 days).</p> <p>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</p>
<i>quarantinePastSecs</i>	<p>Events with timestamp of <code>quarantinePastSecs</code> older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days).</p> <p>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</p>
<i>rawChunkSizeBytes</i>	<p>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, <code>rawChunkSizeBytes</code> is set to the default value.</p> <p><b>Note:</b> <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</p> <p><b>Warning:</b> This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</p>
<i>rotatePeriodInSecs</i>	<p>Rotation period, in seconds, that specifies how frequently to check:</p> <ul style="list-style-type: none"> <li>• If a new hot bucket needs to be created.</li> <li>• If there are any cold buckets that should be frozen.</li> <li>• If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</li> </ul>
<i>serviceMetaPeriod</i>	Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).

Name	Description
	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.
<i>summarize</i>	If true, leaves out certain index details, which provides a faster response.
<i>suppressBannerList</i>	List of indexes for which we suppress "index missing" warning banner messages.  This is a global setting, not a per index setting.
<i>sync</i>	Specifies the number of events that trigger the indexer to sync events.  This is a global setting, not a per index setting.
<i>syncMeta</i>	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.  <i>Note:</i> Do not change this parameter without the input of Splunk Support.
<i>thawedPath</i>	An absolute path that contains the thawed (resurrected) databases for the index.
<i>thawedPath_expanded</i>	Absolute filepath to the thawed (resurrected) databases.
<i>throttleCheckPeriod</i>	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).  <i>Note:</i> Do not change this parameter without the input of Splunk Support.
<i>totalEventCount</i>	Total number of events in the index.

## 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">${SPLUNK_DB}/audit/coldddb</s:key>
    <s:key name="coldPath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/coldddb</s:key>
    <s:key name="coldToFrozenDir"/>
    <s:key name="coldToFrozenScript"/>
    <s:key name="compressRawdata">1</s:key>
    <s:key name="currentDBSizeMB">1</s:key>
    <s:key name="datatype">event</s:key>
    <s:key name="defaultDatabase">main</s:key>
    <s:key name="disabled">0</s:key>
    ... eai:acl element elided ...
    <s:key name="enableRealtimeSearch">1</s:key>
    <s:key name="frozenTimePeriodInSecs">188697600</s:key>
    <s:key name="homePath">${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
<i>blockSignSize</i>	Number	0	<p>Controls how many events make up a block for block signatures.</p> <p>If this is set to 0, block signing is disabled for this index.</p> <p>A recommended value is 100.</p>
<i>bucketRebuildMemoryHint</i>	String	auto	<p>Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.</p> <p><i>Caution:</i> This is an advanced parameter. Inappropriate use of this parameter causes splunkd to not start if rebuild is required. <i>Do not set this parameter unless instructed by Splunk Support.</i></p> <p>Default value, <code>auto</code>, varies by the amount of physical RAM on the host</p> <ul style="list-style-type: none"><li>• less than 2GB RAM = 67108864 (64MB) tsidx</li><li>• 2GB to 8GB RAM = 134217728 (128MB) tsidx</li><li>• more than 8GB RAM = 268435456 (256MB) tsidx</li></ul> <p>Values other than "auto" must be 16MB-1GB. Highest legal value (of the numerical part) is 4294967295</p> <p>You can specify the value using a size suffix: "16777216" or "16MB" are equivalent.</p>
<i>coldPath</i>	String		<p>An absolute path that contains the colddbbs 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).</p> <p>Required. Splunk software does not start if an index lacks a valid coldPath.</p>
<i>coldToFrozenDir</i>	String		<p>Destination path for the frozen archive. Use as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</p> <p>Bucket freezing policy is as follows:</p> <ul style="list-style-type: none"><li>• New style buckets (4.2 and on): removes all files but the rawdata</li></ul> <p>To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</p> <ul style="list-style-type: none"><li>• Old style buckets (Pre-4.2): gzip all the .data and .tsidx files</li></ul> <p>To thaw, gunzip the zipped files and move the bucket into the thawed directory</p>

Name	Type	Default	Description
			If both <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> are specified, <code>coldToFrozenDir</code> takes precedence
<code>coldToFrozenScript</code>	String		<p>Path to the archiving script.</p> <p>If your script requires a program to run it (for example, python), specify the program followed by the path. The script must be in <code>\$SPLUNK_HOME/bin</code> or one of its subdirectories.</p> <p>Splunk software ships with an example archiving script in <code>\$SPLUNK_HOME/bin</code> called <code>coldToFrozenExample.py</code>. DO NOT use this example script directly. It uses a default path, and if modified in place any changes are overwritten on upgrade.</p> <p>It is best to copy the example script to a new file in <code>bin</code> and modify it for your system. Most importantly, change the default archive path to an existing directory that fits your needs.</p> <p>If your new script in <code>bin/</code> is named <code>myColdToFrozen.py</code>, set this key to the following:</p> <pre>coldToFrozenScript = "\$SPLUNK_HOME/bin/python" "\$SPLUNK_HOME/bin/myColdToFrozen.py"</pre> <p>By default, the example script has two possible behaviors when archiving:</p> <ul style="list-style-type: none"> <li>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 <code>splunk rebuild .</code>, then copy the bucket to thawed for that index. We recommend using the <code>coldToFrozenDir</code> parameter unless you need to perform a more advanced operation upon freezing buckets.</li> <li>For older-style buckets, we simply gzip all the <code>.tsidx</code> files. To thaw: cd to the frozen bucket and unzip the <code>tsidx</code> files, then copy the bucket to thawed for that index</li> </ul>
<code>compressRawdata</code>	Boolean	true	This parameter is ignored. The <code>splunkd</code> process always compresses raw data.
<code>datatype</code>	String	event	Valid values: (event   metric). Specifies the type of index.
<code>enableOnlineBucketRepair</code>	Boolean	true	<p>Enables asynchronous "online fsck" bucket repair, which runs concurrently with Splunk software.</p> <p>When enabled, you do not have to wait until buckets are repaired to start the Splunk platform. However, you might observe a slight performance degradation.</p>
<code>frozenTimePeriodInSecs</code>	Number	188697600	<p>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</p> <p>Freezing data means it is removed from the index. If you need to archive your data, refer to <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> parameter documentation.</p>
<code>homePath</code>	String		An absolute path that contains the hot and warm buckets for the index.

Name	Type	Default	Description
			<p>Required. Splunk software does not start if an index lacks a valid homePath.</p> <p><b>Caution:</b> The path must be readable and writable.</p>
<i>maxBloomBackfillBucketAge</i>	Number	30d	<p>Valid values are: Integer[m s h d]</p> <p>If a warm or cold bucket is older than the specified age, do not create or rebuild its Bloom filter. Specify 0 to never rebuild Bloom filters.</p> <p>For example, if a bucket is older than specified with maxBloomBackfillBucketAge, and the rebuilding of its Bloom filter started but did not finish, do not rebuild it.</p>
<i>maxConcurrentOptimizes</i>	Number	6	<p>The number of concurrent optimize processes that can run against a hot bucket.</p> <p>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</p>
<i>maxDataSize</i>	Number	auto	<p>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.</p> <ul style="list-style-type: none"> <li>"auto" sets the size to 750MB.</li> <li>"auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</li> </ul> <p>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.</p> <p>If you specify an invalid number or string, maxDataSize is auto-tuned.</p> <p><i>Note:</i> The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.</p>
<i>maxHotBuckets</i>	Number	3	<p>Maximum hot buckets that can exist per index. Defaults to 3.</p> <p>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.</p>
<i>maxHotIdleSecs</i>	Number	0	<p>Maximum life, in seconds, of a hot bucket. Defaults to 0.</p> <p>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).</p>

Name	Type	Default	Description
<i>maxHotSpanSecs</i>	Number	7776000	<p>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).</p> <p><b>Note:</b> If 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.</p>
<i>maxMemMB</i>	Number	5	<p>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.</p> <p><b>IMPORTANT:</b> Calculate this number carefully. Setting this number incorrectly may have adverse effects on your systems memory and/or splunkd stability/performance.</p>
<i>maxMetaEntries</i>	Number	1000000	<p>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).</p> <p>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 <code>punct</code> field in your data. If you do not use <code>punct</code>, it may be best to simply disable this (see <code>props.conf.spec</code> in <code>\$SPLUNK_HOME/etc/system/README</code>).</p> <p>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.</p>
<i>maxTimeUnreplicatedNoAcks</i>	Number	300	<p>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.</p> <p>If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, <code>maxTimeUnreplicatedWithAcks</code> applies.</p> <p>Highest legal value is 2147483647. To disable this parameter, set to 0.</p> <p><b>Note:</b> this is an advanced parameter. Understand the consequences before changing.</p>
<i>maxTimeUnreplicatedWithAcks</i>	Number	60	<p>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).</p> <p><b>Note:</b> 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 <code>outputs.conf</code> <code>readTimeout</code> setting under the <code>tcpout</code> stanza.</p>

Name	Type	Default	Description
			To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.
<i>maxTotalDataSizeMB</i>	Number	500000	The maximum size of an index (in MB). If an index grows larger than the maximum size, the oldest data is frozen.
<i>maxWarmDBCount</i>	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.
<i>minRawFileSyncSecs</i>	Number	disable	<p>Specify an integer (or "disable") for this parameter.</p> <p>This parameter sets how frequently splunkd forces a filesystem sync while compressing journal slices.</p> <p>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.</p> <p>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.</p> <p><i>Note:</i> Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed</p>
<i>minStreamGroupQueueSize</i>	Number	2000	<p>Minimum size of the queue that stores events in memory before committing them to a tsidx file.</p> <p><i>Caution:</i> Do not set this value, except under advice from Splunk Support.</p>
<i>name</i> required	String		The name of the index to create.
<i>partialServiceMetaPeriod</i>	Number	0	<p>Related to serviceMetaPeriod. If set, it enables metadata sync every &lt;integer&gt; 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.</p> <p><i>partialServiceMetaPeriod</i> 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.</p> <p>If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</p> <p>By default it is turned off (zero).</p>
<i>processTrackerServiceInterval</i>	Number	1	<p>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.</p> <p>If set to 0, the indexer checks child process status every second.</p> <p>Highest legal value is 4294967295.</p>



Name	Type	Default	Description
<i>quarantineFutureSecs</i>	Number	2592000	<p>Events with timestamp of <code>quarantineFutureSecs</code> newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days).</p> <p>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</p>
<i>quarantinePastSecs</i>	Number	77760000	<p>Events with timestamp of <code>quarantinePastSecs</code> older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days).</p> <p>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</p>
<i>rawChunkSizeBytes</i>	Number	131072	<p>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, <code>rawChunkSizeBytes</code> is set to the default value.</p> <p><i>Note:</i> <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</p> <p><b>WARNING:</b> This is an advanced parameter. Only change it if you are instructed to do so by Splunk Support.</p>
<i>repFactor</i>	String	0	<p>Index replication control. This parameter applies to only clustering slaves.</p> <p><code>auto</code> = Use the master index replication configuration value.</p> <p>0 = Turn off replication for this index.</p>
<i>rotatePeriodInSecs</i>	Number	60	<p>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.</p>
<i>serviceMetaPeriod</i>	Number	25	<p>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</p> <p>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.</p>
<i>syncMeta</i>	Boolean	true	<p>When <code>true</code>, 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.</p> <p><b>Note:</b> Do not change this parameter without the input of a Splunk Support.</p>
<i>thawedPath</i>	String		<p>An absolute path that contains the thawed (resurrected) databases for the index.</p> <p>Cannot be defined in terms of a volume definition.</p> <p>Required. Splunk software does not start if an index lacks a valid <code>thawedPath</code>.</p>

Name	Type	Default	Description
<i>throttleCheckPeriod</i>	Number	15	<p>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).</p> <p><b>Note:</b> Do not change this parameter without the input of Splunk Support.</p>
<i>tstatsHomePath</i>	String		<p>Location to store datamodel acceleration TSIDX data for this index. Restart splunkd after changing this parameter.</p> <p>If specified, it must be defined in terms of a volume definition.</p> <p><i>Caution:</i> Path must be writable.</p> <p><i>Default value:</i> volume:_splunk_summaries/\$_index_name/tstats</p>
<i>warmToColdScript</i>	String		<p>Path to a script to run when moving data from warm to cold.</p> <p>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.</p> <p><i>Caution:</i> 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.</p>

#### Returned values

Name	Description
<i>assureUTF8</i>	<p>Boolean value indicating wheter all data retrieved from the index is proper UTF8.</p> <p>If enabled (set to True), degrades indexing performance</p> <p>Can only be set globally.</p>
<i>blockSignSize</i>	<p>Controls how many events make up a block for block signatures.</p> <p>If this is set to 0, block signing is disabled for this index.</p> <p>A recommended value is 100.</p>
<i>blockSignatureDatabase</i>	<p>The index that stores block signatures of events.</p> <p>This is a global setting, not a per index setting.</p>
<i>bucketRebuildMemoryHint</i>	Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.
<i>coldPath</i>	Filepath to the cold databases for the index.
<i>coldPath_expanded</i>	Absoute filepath to the cold databases.
<i>coldToFrozenDir</i>	Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.

Name	Description
	<p>Bucket freezing policy is as follows:</p> <ul style="list-style-type: none"> <li>• New style buckets (4.2 and on): removes all files but the rawdata</li> </ul> <p>To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</p> <ul style="list-style-type: none"> <li>• Old style buckets (Pre-4.2): gzip all the .data and .tsidx files</li> </ul> <p>To thaw, unzip the zipped files and move the bucket into the thawed directory</p> <p>If both <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> are specified, <code>coldToFrozenDir</code> takes precedence.</p>
<i>coldToFrozenScript</i>	<p>Path to the archiving script.</p> <p>See the POST parameter description for details.</p>
<i>compressRawdata</i>	This value is ignored. <code>splunkd</code> process always compresses raw data.
<i>currentDBSizeMB</i>	Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.
<i>datatype</i>	The type of index (event   metric).
<i>defaultDatabase</i>	If no index destination information is available in the input data, the index shown here is the destination of such data.
<i>enableOnlineBucketRepair</i>	Indicates whether to run asynchronous "online fsck" bucket repair, which runs in a process concurrently with Splunk software.
<i>enableRealtimeSearch</i>	<p>Indicates if this is a real-time search.</p> <p>This is a global setting, not a per index setting.</p>
<i>frozenTimePeriodInSecs</i>	<p>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</p> <p>Freezing data means it is removed from the index. If you need to archive your data, refer to <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> parameter documentation.</p>
<i>homePath</i>	An absolute path that contains the hot and warm buckets for the index.
<i>homePath_expanded</i>	An absolute filepath to the hot and warm buckets for the index.
<i>indexThreads</i>	<p>Number of threads used for indexing.</p> <p>This is a global setting, not a per index setting.</p>
<i>isInternal</i>	Indicates if this is an internal index (for example, <code>_internal</code> , <code>_audit</code> ).
<i>isReady</i>	Indicates if an index is properly initialized.
<i>lastInitTime</i>	<p>Last time the index processor was successfully initialized.</p> <p>This is a global setting, not a per index setting.</p>
<i>maxBloomBackfillBucketAge</i>	If a bucket (warm or cold) is older than this, Splunk software does not create (or re-create) its Bloom filter.
<i>maxConcurrentOptimizes</i>	<p>The number of concurrent optimize processes that can run against a hot bucket.</p> <p>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</p>

Name	Description
<i>maxDataSize</i>	<p>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.</p> <ul style="list-style-type: none"> <li>• "auto" sets the size to 750MB.</li> <li>• "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</li> </ul> <p>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.</p> <p>If you specify an invalid number or string, maxDataSize is auto-tuned.</p> <p><i>Note:</i> The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.</p>
<i>maxHotBuckets</i>	<p>Maximum hot buckets that can exist per index. Defaults to 3.</p> <p>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.</p>
<i>maxHotIdleSecs</i>	<p>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).</p> <p>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.</p>
<i>maxHotSpanSecs</i>	<p>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).</p> <p><i>Note:</i> 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.</p>
<i>maxMemMB</i>	<p>The amount of memory, in MB, allocated for indexing.</p> <p>This is a global setting, not a per index setting.</p>
<i>maxMetaEntries</i>	<p>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).</p> <p>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).</p> <p>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.</p>

Name	Description
<i>maxTime</i>	ISO8601 timestamp of the newest event time in the index.
<i>maxTimeUnreplicatedNoAcks</i>	<p>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.</p> <p>If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, <i>maxTimeUnreplicatedWithAcks</i> applies.</p> <p>Highest legal value is 2147483647. To disable this parameter, set to 0.</p> <p><i>Note:</i> this is an advanced parameter. Understand the consequences before changing.</p>
<i>maxTimeUnreplicatedWithAcks</i>	<p>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).</p> <p><i>Note:</i> 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 <code>outputs.conf</code> <code>readTimeout</code> setting under the <code>tcpout</code> stanza.</p> <p>To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.</p>
<i>maxTotalDataSizeMB</i>	The maximum size of an index, in MB.
<i>maxWarmDBCount</i>	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.
<i>memPoolMB</i>	<p>Determines how much memory is given to the indexer memory pool.</p> <p>This is a global setting, not a per-index setting.</p>
<i>minRawFileSyncSecs</i>	<p>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</p> <p>The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices.</p> <p>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.</p> <p>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.</p>
<i>minStreamGroupQueueSize</i>	Minimum size of the queue that stores events in memory before committing them to a <code>tsidx</code> file.
<i>minTime</i>	ISO8601 timestamp of the oldest event time in the index.
<i>partialServiceMetaPeriod</i>	<p>Related to <code>serviceMetaPeriod</code>. By default it is turned off (zero).</p> <p>If set, it enables metadata sync every <code>&lt;integer&gt;</code> 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 <code>serviceMetaPeriod</code>.</p>

Name	Description
	<p>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.</p> <p>If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</p>
<i>processTrackerServiceInterval</i>	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.
<i>quarantineFutureSecs</i>	<p>Events with timestamp of quarantineFutureSecs newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days).</p> <p>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</p>
<i>quarantinePastSecs</i>	<p>Events with timestamp of quarantinePastSecs older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days).</p> <p>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</p>
<i>rawChunkSizeBytes</i>	<p>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.</p> <p><b>Note:</b> rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</p> <p><b>Warning:</b> This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</p>
<i>repFactor</i>	<p>Index replication control. This parameter applies to only clustering slaves.</p> <p>auto = Use the master index replication configuration value.</p> <p>0 = Turn off replication for this index.</p>
<i>rotatePeriodInSecs</i>	<p>Rotation period, in seconds, that specifies how frequently to check:</p> <ul style="list-style-type: none"> <li>• If a new hot bucket needs to be created.</li> <li>• If there are any cold buckets that should be frozen.</li> <li>• If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</li> </ul>
<i>serviceMetaPeriod</i>	<p>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</p> <p>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.</p>
<i>suppressBannerList</i>	<p>List of indexes for which we suppress "index missing" warning banner messages.</p> <p>This is a global setting, not a per index setting.</p>
<i>sync</i>	<p>Specifies the number of events that trigger the indexer to sync events.</p> <p>This is a global setting, not a per index setting.</p>
<i>syncMeta</i>	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.

Name	Description
	<b>Note:</b> Do not change this parameter without the input of Splunk Support.
<i>thawedPath</i>	Filepath to the thawed (resurrected) databases for the index.
<i>thawedPath_expanded</i>	Absolute filepath to the thawed (resurrected) databases.
<i>throttleCheckPeriod</i>	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).  <b>Note:</b> Do not change this parameter without the input of Splunk Support.
<i>totalEventCount</i>	Total number of events in the index.
<i>tstatsHomePath</i>	Location where datamodel acceleration TSIDX data for this index is stored.
<i>warmToColdScript</i>	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:dict>
  </content>
</entry>
</s:messages>
```

```

<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
<i>assureUTF8</i>	<p>Indicates whether all data retrieved from the index is proper UTF8. If enabled (set to True), degrades indexing performance.</p> <p>This is a global setting, not a per index setting.</p>
<i>blockSignSize</i>	<p>Controls how many events make up a block for block signatures.</p> <p>If this is set to 0, block signing is disabled for this index.</p> <p>A recommended value is 100.</p>
<i>blockSignatureDatabase</i>	<p>The index that stores block signatures of events.</p> <p>This is a global setting, not a per index setting.</p>
<i>bloomfilterTotalSizeKB</i>	Total size of all Bloom filter files, in KB.
<i>coldPath</i>	Filepath to the cold databases for the index.
<i>coldPath_expanded</i>	Absolute filepath to the cold databases.
<i>coldToFrozenDir</i>	<p>Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</p> <p>Bucket freezing policy is as follows:</p> <ul style="list-style-type: none"> <li>• New style buckets (4.2 and on): removes all files but the rawdata <p>To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</p> </li> <li>• Old style buckets (Pre-4.2): gzip all the .data and .tsidx files <p>To thaw, unzip the zipped files and move the bucket into the thawed directory</p> </li> </ul> <p>If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.</p>
<i>coldToFrozenScript</i>	<p>Path to the archiving script.</p> <p>See the POST parameter description for details.</p>
<i>compressRawdata</i>	This value is ignored. splunkd process always compresses raw data.
<i>currentDBSizeMB</i>	Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.
<i>defaultDatabase</i>	If no index destination information is available in the input data, the index shown here is the destination of such data.
<i>disabled</i>	Indicates if the index is disabled.
<i>enableRealtimeSearch</i>	<p>Indicates if this is a real-time search.</p> <p>This is a global setting, not a per index setting.</p>
<i>frozenTimePeriodInSecs</i>	<p>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</p> <p>Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.</p>

Name	Description
<i>homePath</i>	An absolute path that contains the hot and warm buckets for the index.
<i>homePath_expanded</i>	An absolute filepath to the hot and warm buckets for the index.
<i>indexThreads</i>	Number of threads used for indexing.  This is a global setting, not a per index setting.
<i>isInternal</i>	Indicates if this is an internal index (for example, <i>_internal</i> , <i>_audit</i> ).
<i>lastInitTime</i>	Last time the index processor was successfully initialized.  This is a global setting, not a per index setting.
<i>maxConcurrentOptimizes</i>	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.
<i>maxDataSize</i>	<p>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.</p> <ul style="list-style-type: none"> <li>• "auto" sets the size to 750MB.</li> <li>• "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</li> </ul> <p>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.</p> <p>If you specify an invalid number or string, maxDataSize is auto-tuned.</p> <p><i>Note:</i> The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.</p>
<i>maxHotBuckets</i>	<p>Maximum hot buckets that can exist per index. Defaults to 3.</p> <p>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.</p>
<i>maxHotIdleSecs</i>	<p>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).</p> <p>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.</p>
<i>maxHotSpanSecs</i>	<p>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).</p> <p><i>Note:</i> 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.</p>

Name	Description
<i>maxMemMB</i>	<p>The amount of memory, in MB, allocated for indexing.</p> <p>This is a global setting, not a per index setting.</p>
<i>maxMetaEntries</i>	<p>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).</p> <p>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).</p> <p>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.</p>
<i>maxRunningProcessGroups</i>	<p>Maximum number of processes that the indexer fires off at a time.</p> <p>This is a global setting, not a per index setting.</p>
<i>maxTime</i>	UNIX timestamp of the newest event time in the index.
<i>maxTotalDataSizeMB</i>	The maximum size of an index, in MB.
<i>maxWarmDBCount</i>	Maximum number of warm buckets.
<i>memPoolMB</i>	<p>Determines how much memory is given to the indexer memory pool.</p> <p>This is a global setting, not a per-index setting.</p>
<i>minRawFileSyncSecs</i>	<p>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</p> <p>The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices.</p> <p>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.</p> <p>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.</p>
<i>minTime</i>	UNIX timestamp of the oldest event time in the index.
<i>numBloomfilters</i>	The number of Bloom filters created for this index.
<i>numHotBuckets</i>	The number of hot buckets created for this index.
<i>numWarmBuckets</i>	The number of warm buckets created for this index.
<i>partialServiceMetaPeriod</i>	<p>Related to serviceMetaPeriod. By default it is turned off (zero).</p> <p>If set, it enables metadata sync every &lt;integer&gt; 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</p>

Name	Description
	<p>that require full re-write are be sync'ed at serviceMetaPeriod.</p> <p>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.</p> <p>If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</p>
<i>quarantineFutureSecs</i>	<p>Events with timestamp of <code>quarantineFutureSecs</code> newer than "now" that are dropped into quarantine bucket. Defaults to 2592000 (30 days).</p> <p>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</p>
<i>quarantinePastSecs</i>	<p>Events with timestamp of <code>quarantinePastSecs</code> older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days).</p> <p>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</p>
<i>rawChunkSizeBytes</i>	<p>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, <code>rawChunkSizeBytes</code> is set to the default value.</p> <p><b>Note:</b> <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</p> <p><b>Warning:</b> This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</p>
<i>rotatePeriodInSecs</i>	<p>Rotation period, in seconds, that specifies how frequently to check:</p> <ul style="list-style-type: none"> <li>• If a new hot bucket needs to be created.</li> <li>• If there are any cold buckets that should be frozen.</li> <li>• If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</li> </ul>
<i>serviceMetaPeriod</i>	<p>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</p> <p>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.</p>
<i>summarize</i>	If true, leaves out certain index details, which provides a faster response.
<i>suppressBannerList</i>	<p>List of indexes for which we suppress "index missing" warning banner messages.</p> <p>This is a global setting, not a per index setting.</p>
<i>sync</i>	<p>Specifies the number of events that trigger the indexer to sync events.</p> <p>This is a global setting, not a per index setting.</p>
<i>syncMeta</i>	<p>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.</p> <p><b>Note:</b> Do not change this parameter without the input of Splunk Support.</p>
<i>thawedPath</i>	An absolute path that contains the thawed (resurrected) databases for the index.
<i>thawedPath_expanded</i>	Absolute filepath to the thawed (resurrected) databases.

Name	Description
<i>throttleCheckPeriod</i>	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).  <i>Note:</i> Do not change this parameter without the input of Splunk Support.
<i>totalEventCount</i>	Total number of events in the index.

## 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
<i>blockSignSize</i>	Number	0	<p>Controls how many events make up a block for block signatures.</p> <p>If this is set to 0, block signing is disabled for this index.</p> <p>A recommended value is 100.</p>
<i>bucketRebuildMemoryHint</i>	String	auto	<p>Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.</p> <p><b>Caution:</b> This is an advanced parameter. Inappropriate use of this parameter causes splunkd to not start if rebuild is required. <i>Do not set this parameter unless instructed by Splunk Support.</i></p> <p>Default value, <code>auto</code>, varies by the amount of physical RAM on the host</p> <ul style="list-style-type: none"> <li>less than 2GB RAM = 67108864 (64MB) tsidx</li> <li>2GB to 8GB RAM = 134217728 (128MB) tsidx</li> <li>more than 8GB RAM = 268435456 (256MB) tsidx</li> </ul> <p>Values other than "auto" must be 16MB-1GB. Highest legal value (of the numerical part) is 4294967295</p> <p>You can specify the value using a size suffix: "16777216" or "16MB" are equivalent.</p>
<i>coldToFrozenDir</i>	String		<p>Destination path for the frozen archive. Use as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</p> <p>Bucket freezing policy is as follows:</p>



Name	Type	Default	Description
			<ul style="list-style-type: none"> <li>• New style buckets (4.2 and on): removes all files but the rawdata</li> </ul> <p>To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</p> <ul style="list-style-type: none"> <li>• Old style buckets (Pre-4.2): gzip all the .data and .tsidx files</li> </ul> <p>To thaw, gunzip the zipped files and move the bucket into the thawed directory</p> <p>If both <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> are specified, <code>coldToFrozenDir</code> takes precedence</p>
<i>coldToFrozenScript</i>	String		<p>Path to the archiving script.</p> <p>If your script requires a program to run it (for example, python), specify the program followed by the path. The script must be in <code>\$SPLUNK_HOME/bin</code> or one of its subdirectories.</p> <p>Splunk software ships with an example archiving script in <code>\$SPLUNK_HOME/bin</code> called <code>coldToFrozenExample.py</code>. DO NOT use this example script directly. It uses a default path, and if modified in place any changes are overwritten on upgrade.</p> <p>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.</p> <p>If your new script in bin/ is named <code>myColdToFrozen.py</code>, set this key to the following:</p> <pre>coldToFrozenScript = "\$SPLUNK_HOME/bin/python" "\$SPLUNK_HOME/bin/myColdToFrozen.py"</pre> <p>By default, the example script has two possible behaviors when archiving:</p> <ul style="list-style-type: none"> <li>• 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 <code>splunk rebuild .</code>, then copy the bucket to thawed for that index. We recommend using the <code>coldToFrozenDir</code> parameter unless you need to perform a more advanced operation upon freezing buckets.</li> <li>• 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</li> </ul>
<i>compressRawdata</i>	Boolean	true	This parameter is ignored. The splunkd process always compresses raw data.
<i>enableOnlineBucketRepair</i>	Boolean	true	<p>Enables asynchronous "online fsck" bucket repair, which runs concurrently with Splunk software.</p> <p>When enabled, you do not have to wait until buckets are repaired to start Splunk Enterprise. However, you might observe a slight performance degratation.</p>

Name	Type	Default	Description
<i>frozenTimePeriodInSecs</i>	Number	188697600	<p>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</p> <p>Freezing data means it is removed from the index. If you need to archive your data, refer to <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> parameter documentation.</p>
<i>maxBloomBackfillBucketAge</i>	Number	30d	<p>Valid values are: Integer[m s h d]</p> <p>If a warm or cold bucket is older than the specified age, do not create or rebuild its Bloom filter. Specify 0 to never rebuild Bloom filters.</p> <p>For example, if a bucket is older than specified with <code>maxBloomBackfillBucketAge</code>, and the rebuilding of its Bloom filter started but did not finish, do not rebuild it.</p>
<i>maxConcurrentOptimizes</i>	Number	6	<p>The number of concurrent optimize processes that can run against a hot bucket.</p> <p>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</p>
<i>maxDataSize</i>	Number	auto	<p>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.</p> <ul style="list-style-type: none"> <li>• "auto" sets the size to 750MB.</li> <li>• "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</li> </ul> <p>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.</p> <p>If you specify an invalid number or string, <code>maxDataSize</code> is auto-tuned.</p> <p><i>Note:</i> The precise size of your warm buckets may vary from <code>maxDataSize</code>, due to post-processing and timing issues with the rolling policy.</p>
<i>maxHotBuckets</i>	Number	3	<p>Maximum hot buckets that can exist per index. Defaults to 3.</p> <p>When <code>maxHotBuckets</code> 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 <code>maxHotIdleSecs</code>, which can also cause hot buckets to roll.</p>
<i>maxHotIdleSecs</i>	Number	0	<p>Maximum life, in seconds, of a hot bucket. Defaults to 0.</p>

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).
<i>maxHotSpanSecs</i>	Number	7776000	Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).  <i>Note:</i> If 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.
<i>maxMemMB</i>	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.  <b>IMPORTANT:</b> Calculate this number carefully. Setting this number incorrectly may have adverse effects on your systems memory and/or splunkd stability/performance.
<i>maxMetaEntries</i>	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 <code>punct</code> 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.
<i>maxTimeUnreplicatedNoAcks</i>	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 parameter does not apply. In this case, maxTimeUnreplicatedWithAcks applies.  Highest legal value is 2147483647. To disable this parameter, set to 0.  <i>Note:</i> this is an advanced parameter. Understand the consequences before changing.
<i>maxTimeUnreplicatedWithAcks</i>	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).  <i>Note:</i> 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
			<p>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.</p> <p>To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.</p>
<i>maxTotalDataSizeMB</i>	Number	500000	The maximum size of an index (in MB). If an index grows larger than the maximum size, the oldest data is frozen.
<i>maxWarmDBCount</i>	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.
<i>minRawFileSyncSecs</i>	Number	disable	<p>Specify an integer (or "disable") for this parameter.</p> <p>This parameter sets how frequently splunkd forces a filesystem sync while compressing journal slices.</p> <p>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.</p> <p>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.</p> <p><i>Note:</i> Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed</p>
<i>minStreamGroupQueueSize</i>	Number	2000	<p>Minimum size of the queue that stores events in memory before committing them to a tsidx file.</p> <p><i>Caution:</i> Do not set this value, except under advice from Splunk Support.</p>
<i>partialServiceMetaPeriod</i>	Number	0	<p>Related to serviceMetaPeriod. If set, it enables metadata sync every &lt;integer&gt; 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'd at serviceMetaPeriod.</p> <p><i>partialServiceMetaPeriod</i> 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.</p> <p>If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</p> <p>By default it is turned off (zero).</p>
<i>processTrackerServiceInterval</i>	Number	1	<p>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.</p> <p>If set to 0, the indexer checks child process status every second.</p>

Name	Type	Default	Description
			Highest legal value is 4294967295.
<i>quarantineFutureSecs</i>	Number	2592000	<p>Events with timestamp of <code>quarantineFutureSecs</code> newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days).</p> <p>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</p>
<i>quarantinePastSecs</i>	Number	77760000	<p>Events with timestamp of <code>quarantinePastSecs</code> older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days).</p> <p>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</p>
<i>rawChunkSizeBytes</i>	Number	131072	<p>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, <code>rawChunkSizeBytes</code> is set to the default value.</p> <p><b>Note:</b> <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</p> <p><b>WARNING:</b> This is an advanced parameter. Only change it if you are instructed to do so by Splunk Support.</p>
<i>repFactor</i>	String	0	<p>Index replication control. This parameter applies to only clustering slaves.</p> <p><code>auto</code> = Use the master index replication configuration value.</p> <p>0 = Turn off replication for this index.</p>
<i>rotatePeriodInSecs</i>	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.
<i>serviceMetaPeriod</i>	Number	25	<p>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</p> <p>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.</p>
<i>syncMeta</i>	Boolean	true	<p>When <code>true</code>, 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.</p> <p><b>Note:</b> Do not change this parameter without the input of a Splunk Support.</p>
<i>throttleCheckPeriod</i>	Number	15	<p>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).</p> <p><b>Note:</b> Do not change this parameter without the input of Splunk Support.</p>
<i>tstatsHomePath</i>	String		

Name	Type	Default	Description
			<p>Location to store datamodel acceleration TSIDX data for this index. Restart splunkd after changing this parameter.</p> <p>If specified, it must be defined in terms of a volume definition.</p> <p><i>Caution:</i> Path must be writable.</p> <p><i>Default value:</i> volume:_splunk_summaries/\$_index_name/tstats</p>
<i>warmToColdScript</i>	String		<p>Path to a script to run when moving data from warm to cold.</p> <p>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.</p> <p><i>Caution:</i> 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.</p>

#### Returned values

Name	Description
<i>assureUTF8</i>	<p>Boolean value indicating wheter all data retrieved from the index is proper UTF8.</p> <p>If enabled (set to True), degrades indexing performance</p> <p>Can only be set globally.</p>
<i>blockSignSize</i>	<p>Controls how many events make up a block for block signatures.</p> <p>If this is set to 0, block signing is disabled for this index.</p> <p>A recommended value is 100.</p>
<i>blockSignatureDatabase</i>	<p>The index that stores block signatures of events.</p> <p>This is a global setting, not a per index setting.</p>
<i>bucketRebuildMemoryHint</i>	Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.
<i>coldPath</i>	Filepath to the cold databases for the index.
<i>coldPath_expanded</i>	Absolute filepath to the cold databases.
<i>coldToFrozenDir</i>	<p>Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk Enterprise automatically puts frozen buckets in this directory.</p> <p>Bucket freezing policy is as follows:</p> <ul style="list-style-type: none"> <li>• New style buckets (4.2 and on): removes all files but the rawdata</li> </ul> <p>To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</p> <ul style="list-style-type: none"> <li>• Old style buckets (Pre-4.2): gzip all the .data and .tsidx files</li> </ul>

Name	Description
	<p>To thaw, gunzip the zipped files and move the bucket into the thawed directory</p> <p>If both <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> are specified, <code>coldToFrozenDir</code> takes precedence.</p>
<code>coldToFrozenScript</code>	<p>Path to the archiving script.</p> <p>See the POST parameter description for details.</p>
<code>compressRawdata</code>	This value is ignored. splunkd process always compresses raw data.
<code>currentDBSizeMB</code>	Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.
<code>defaultDatabase</code>	If no index destination information is available in the input data, the index shown here is the destination of such data.
<code>enableOnlineBucketRepair</code>	Indicates whether to run asynchronous "online fsck" bucket repair, which runs in a process concurrently with Splunk software.
<code>enableRealtimeSearch</code>	<p>Indicates if this is a real-time search.</p> <p>This is a global setting, not a per index setting.</p>
<code>frozenTimePeriodInSecs</code>	<p>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</p> <p>Freezing data means it is removed from the index. If you need to archive your data, refer to <code>coldToFrozenDir</code> and <code>coldToFrozenScript</code> parameter documentation.</p>
<code>homePath</code>	An absolute path that contains the hot and warm buckets for the index.
<code>homePath_expanded</code>	An absolute filepath to the hot and warm buckets for the index.
<code>indexThreads</code>	<p>Number of threads used for indexing.</p> <p>This is a global setting, not a per index setting.</p>
<code>isInternal</code>	Indicates if this is an internal index (for example, <code>_internal</code> , <code>_audit</code> ).
<code>lastInitTime</code>	<p>Last time the index processor was successfully initialized.</p> <p>This is a global setting, not a per index setting.</p>
<code>maxBloomBackfillBucketAge</code>	If a bucket (warm or cold) is older than this, Splunk Enterprise does not create (or re-create) its Bloom filter.
<code>maxConcurrentOptimizes</code>	<p>The number of concurrent optimize processes that can run against a hot bucket.</p> <p>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</p>
<code>maxDataSize</code>	<p>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.</p> <ul style="list-style-type: none"> <li>• "auto" sets the size to 750MB.</li> <li>• "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</li> </ul> <p>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</p>

Name	Description
	<p>should be approved by Splunk Support before proceeding.</p> <p>If you specify an invalid number or string, <code>maxDataSize</code> is auto-tuned.</p> <p><i>Note:</i> The precise size of your warm buckets may vary from <code>maxDataSize</code>, due to post-processing and timing issues with the rolling policy.</p>
<i>maxHotBuckets</i>	<p>Maximum hot buckets that can exist per index. Defaults to 3.</p> <p>When <code>maxHotBuckets</code> 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 <code>maxHotIdleSecs</code>, which can also cause hot buckets to roll.</p>
<i>maxHotIdleSecs</i>	<p>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).</p> <p>If a hot bucket exceeds <code>maxHotIdleSecs</code>, Splunk software rolls it to warm. This setting operates independently of <code>maxHotBuckets</code>, which can also cause hot buckets to roll.</p>
<i>maxHotSpanSecs</i>	<p>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).</p> <p><i>Note:</i> 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.</p>
<i>maxMemMB</i>	<p>The amount of memory, in MB, allocated for indexing.</p> <p>This is a global setting, not a per index setting.</p>
<i>maxMetaEntries</i>	<p>Sets the maximum number of unique lines in <code>.data</code> files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).</p> <p>If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to <code>Strings.data</code> hitting this limit, the culprit may be the <code>punct</code> field in your data. If you do not use <code>punct</code>, it may be best to simply disable this (see <code>props.conf.spec</code> in <code>\$SPLUNK_HOME/etc/system/README</code>).</p> <p>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.</p>
<i>maxTime</i>	<p>UNIX timestamp of the newest event time in the index.</p>
<i>maxTimeUnreplicatedNoAcks</i>	<p>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.</p> <p>If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, <code>maxTimeUnreplicatedWithAcks</code> applies.</p> <p>Highest legal value is 2147483647. To disable this parameter, set to 0.</p>



Name	Description
	<i>Note:</i> this is an advanced parameter. Understand the consequences before changing.
<i>maxTimeUnreplicatedWithAcks</i>	<p>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).</p> <p><i>Note:</i> 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 topout stanza.</p> <p>To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.</p>
<i>maxTotalDataSizeMB</i>	The maximum size of an index, in MB.
<i>maxWarmDBCount</i>	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.
<i>memPoolMB</i>	<p>Determines how much memory is given to the indexer memory pool.</p> <p>This is a global setting, not a per-index setting.</p>
<i>minRawFileSyncSecs</i>	<p>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</p> <p>The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices.</p> <p>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.</p> <p>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.</p>
<i>minStreamGroupQueueSize</i>	Minimum size of the queue that stores events in memory before committing them to a tsidx file.
<i>minTime</i>	UNIX timestamp of the oldest event time in the index.
<i>partialServiceMetaPeriod</i>	<p>Related to serviceMetaPeriod. By default it is turned off (zero).</p> <p>If set, it enables metadata sync every &lt;integer&gt; 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.</p> <p>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.</p> <p>If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</p>
<i>processTrackerServiceInterval</i>	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.

Name	Description
<i>quarantineFutureSecs</i>	<p>Events with timestamp of <code>quarantineFutureSecs</code> newer than "now" are dropped into quarantine bucket. Defaults to 2592000 (30 days).</p> <p>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</p>
<i>quarantinePastSecs</i>	<p>Events with timestamp of <code>quarantinePastSecs</code> older than "now" are dropped into quarantine bucket. Defaults to 77760000 (900 days).</p> <p>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</p>
<i>rawChunkSizeBytes</i>	<p>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, <code>rawChunkSizeBytes</code> is set to the default value.</p> <p><b>Note:</b> <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</p> <p><b>Warning:</b> This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</p>
<i>repFactor</i>	<p>Index replication control. This parameter applies to only clustering slaves.</p> <p><code>auto</code> = Use the master index replication configuration value.</p> <p><code>0</code> = Turn off replication for this index.</p>
<i>rotatePeriodInSecs</i>	<p>Rotation period, in seconds, that specifies how frequently to check:</p> <ul style="list-style-type: none"> <li>• If a new hot bucket needs to be created.</li> <li>• If there are any cold buckets that should be frozen.</li> <li>• If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</li> </ul>
<i>serviceMetaPeriod</i>	<p>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</p> <p>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.</p>
<i>suppressBannerList</i>	<p>List of indexes for which we suppress "index missing" warning banner messages.</p> <p>This is a global setting, not a per index setting.</p>
<i>sync</i>	<p>Specifies the number of events that trigger the indexer to sync events.</p> <p>This is a global setting, not a per index setting.</p>
<i>syncMeta</i>	<p>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.</p> <p><b>Note:</b> Do not change this parameter without the input of Splunk Support.</p>
<i>thawedPath</i>	Filepath to the thawed (resurrected) databases for the index.
<i>thawedPath_expanded</i>	Absolute filepath to the thawed (resurrected) databases.
<i>throttleCheckPeriod</i>	Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).

Name	Description
	<i>Note:</i> Do not change this parameter without the input of Splunk Support.
<i>totalEventCount</i>	Total number of events in the index.
<i>tstatsHomePath</i>	Location where datamodel acceleration TSIDX data for this index is stored.
<i>warmToColdScript</i>	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
<i>datatype</i>	String	all	Valid values: (all   event   metric). Specifies the type of index.

## Returned values

Name	Description				
bucket_dirs	(If <i>total_size</i> > 0) Lists the following attributes for each index bucket super-directory ( <i>home</i> , <i>cold</i> , <i>thawed</i> ).				
	Attribute	Description	home	cold	thawed
	bucket_count	Number of buckets.		X	X
	event_count	(If <i>size</i> > 0) Number of events in this bucket super-directory.	X	X	X
	event_max_time	(If <i>size</i> > 0) Highest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called <i>latest time</i> .	X	X	X
	event_min_time	(If <i>size</i> > 0) Lowest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called <i>earliest time</i> .	X	X	X
	hot_bucket_count	(If <i>size</i> > 0) Number of hot buckets.	X		
	size	Size (fractional MB) on disk of this bucket super-directory.	X	X	X
	warm_bucket_count	(If <i>size</i> > 0) Number of warm buckets.	X		
name	Index name.				
total_bucket_count	(If <i>total_size</i> > 0) Number of index buckets.				
total_event_count	(If <i>total_size</i> > 0) Number of events for index, excluding <i>frozen</i> events. Approximately equal to the <i>event_count</i> sum of all buckets.				
total_raw_size	(If <i>total_size</i> > 0) Cumulative size (fractional MB) on disk of the <bucket>/rawdata/ directories of all buckets in this index, excluding <i>frozen</i> .				
total_size	Size (fractional MB) on disk of this index.				

## 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

Name	Description				
<i>bucket_dirs</i>	(If <i>total_size</i> > 0) List the following attributes for each index bucket super-directory ( <i>home</i> , <i>cold</i> , <i>thawed</i> ) as indicated:				
	Attribute	Description	home	cold	thawed
	bucket_count	Number of buckets.		X	X
	event_count	(If <i>size</i> > 0) Number of events in this bucket super-directory.	X	X	X
	event_max_time	(If <i>size</i> > 0) Highest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called <i>latest time</i> .	X	X	X
	event_min_time	(If <i>size</i> > 0) Lowest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called <i>earliest time</i> .	X	X	X
	hot_bucket_count	(If <i>size</i> > 0) Number of hot buckets.	X		
	size	Size (fractional MB) on disk of this bucket super-directory.	X	X	X
	warm_bucket_count	(If <i>size</i> > 0) Number of warm buckets.	X		
<i>name</i>	Index name.				
<i>total_bucket_count</i>	(If <i>total_size</i> > 0) Number of index buckets.				
<i>total_event_count</i>	(If <i>total_size</i> > 0) Number of events for index, excluding <i>frozen</i> events. Approximately equal to the <i>event_count</i> sum of all buckets.				
<i>total_raw_size</i>	(If <i>total_size</i> > 0) Cumulative size (fractional MB) on disk of the <bucket>/rawdata/ directories of all buckets in this index, excluding <i>frozen</i> .				
<i>total_size</i>	Size (fractional MB) on disk of this index.				

## 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
<i>report_acceleration</i>	Optional. Use "report_acceleration=1" to access disk usage by report acceleration summary.
<i>data_model_acceleration</i>	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
<i>name</i>	Summary name.
<i>related_indexes</i>	Lists up to 10 indexes that contribute to this summary.
<i>related_indexes_count</i>	Provides total count of related indexes for this summary.
<i>search_head_guid</i>	GUID for the search head that created the summary data.
<i>total_bucket_count</i>	Number of buckets for this summary.
<i>total_size</i>	Total disk size for this summary, in MB.
<i>type</i>	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:dict>
  </content>
</entry>

```

```

</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
<i>name</i>	Summary name.
<i>related_indexes</i>	Lists up to 10 indexes that contribute to this summary.
<i>related_indexes_count</i>	Provides total count of related indexes for this summary.
<i>search_head_guid</i>	GUID for search head creating the summary data.
<i>total_bucket_count</i>	Number of buckets for this summary.
<i>total_size</i>	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="049b19239844e1f7e09be3d55713claae663e7ae" 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
<i>health</i>	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:dict>
    </s:key>
  </s:dict>
</content>
</xml>
```

```

    <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
<i>display_name</i>	String	The name of the feature in the distributed health tree.
<i>health</i>	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.
<i>reason</i>	String	Descriptive string explaining 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://mrt:9808/services/server/health</id>
<updated>2020-02-05T09:07:09-08:00</updated>
<generator build="e7558703e5bae4dc0cf8d06fa773eb1e75e23552" version="20200205"/>
<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://mrt:9808/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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

```

    </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">green</s:key>
    <s:key name="num_red">0</s:key>
    <s:key name="num_yellow">0</s:key>
    <s:key name="splunkd">
      <s:dict>
        <s:key name="file_monitor_input">
          <s:dict>
            <s:key name="batchreader-0">
              <s:dict>
                <s:key name="data_out_rate">
                  <s:dict>
                    <s:key name="description"><![CDATA[This indicator reflects the number of
consecutive times the Batch File Reader was unable to insert data into Splunk's processing queues for a
period of 5 seconds. By default, this indicator becomes Yellow when this input stalls for 5 seconds, Red
after 10 seconds.]]></s:key>
                    <s:key name="name">data_out_rate</s:key>
                    <s:key
name="path">splunkd.file_monitor_input.batchreader-0.data_out_rate</s:key>
                  </s:dict>
                </s:key>
                <s:key name="display_name">Batch Reader</s:key>
                <s:key name="health">green</s:key>
                <s:key name="num_red">0</s:key>
                <s:key name="num_yellow">0</s:key>
              </s:dict>
            </s:key>
            <s:key name="health">green</s:key>
            <s:key name="num_red">0</s:key>
            <s:key name="num_yellow">0</s:key>
            <s:key name="tailreader-0">
              <s:dict>
                <s:key name="data_out_rate">
                  <s:dict>
                    <s:key name="description"><![CDATA[This indicator reflects the number of
consecutive times the Tail File Reader was unable to insert data into Splunk's processing queues for a
period of 5 seconds. By default, this indicator becomes Yellow when this input stalls for 5 seconds, and Red
after 10 seconds.]]></s:key>
                    <s:key name="name">data_out_rate</s:key>
                    <s:key name="path">splunkd.file_monitor_input.tailreader-0.data_out_rate</s:key>
                  </s:dict>
                </s:key>
                <s:key name="display_name">Tail Reader</s:key>
                <s:key name="health">green</s:key>
                <s:key name="num_red">0</s:key>
                <s:key name="num_yellow">0</s:key>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="health">green</s:key>
        <s:key name="index_processor">
          <s:dict>
            <s:key name="buckets">
              <s:dict>
                <s:key name="buckets_created_last_60m">

```

```

        <s:dict>
            <s:key name="description"><![CDATA[This indicator gauges whether incoming data
is being appropriately bucketed within the Splunk index. By default, Red occurs when any index has created
more than 60 buckets within the last hour. A high rate of bucket creation can cause severe search
performance degradation, and might indicate poorly configured data processing (for example,
timestamping).]]></s:key>
            <s:key name="name">buckets_created_last_60m</s:key>
            <s:key
name="path">splunkd.index_processor.buckets.buckets_created_last_60m</s:key>
        </s:dict>
    </s:key>
    <s:key name="display_name">Buckets</s:key>
    <s:key name="health">green</s:key>
    <s:key name="num_red">0</s:key>
    <s:key name="num_yellow">0</s:key>
    <s:key name="percent_small_buckets_created_last_24h">
        <s:dict>
            <s:key name="description">This indicator tracks the percentage of small buckets
created over the last 24 hours. A small bucket is defined as less than 10 % of the 'maxDataSize' setting in
indexes.conf.</s:key>
            <s:key name="name">percent_small_buckets_created_last_24h</s:key>
            <s:key
name="path">splunkd.index_processor.buckets.percent_small_buckets_created_last_24h</s:key>
        </s:dict>
    </s:key>
</s:dict>
</s:key>
<s:key name="disk_space">
    <s:dict>
        <s:key name="disk_space_remaining_multiple_minfreespace">
            <s:dict>
                <s:key name="description"><![CDATA[This indicator tracks whether all Splunk
index filesystems contain sufficient free space to continue indexing. This calculation is based upon the
'minFreeSpace' setting in server.conf. By default, Yellow occurs when a filesystem's free space falls below
(2* 'minFreeSpace'), and Red when it falls below 'minFreeSpace'.]]></s:key>
                <s:key name="name">disk_space_remaining_multiple_minfreespace</s:key>
                <s:key
name="path">splunkd.index_processor.disk_space.disk_space_remaining_multiple_minfreespace</s:key>
            </s:dict>
        </s:key>
        <s:key name="display_name">Disk Space</s:key>
        <s:key name="health">green</s:key>
        <s:key name="num_red">0</s:key>
        <s:key name="num_yellow">0</s:key>
    </s:dict>
</s:key>
<s:key name="health">green</s:key>
<s:key name="index_optimization">
    <s:dict>
        <s:key name="concurrent_optimize_processes_percent">
            <s:dict>
                <s:key name="description">This indicator tracks whether index optimization is
falling behind. By default, this indicator becomes Yellow when 100% of the maximum allowed
"splunk-optimize" processes are running.</s:key>
                <s:key name="name">concurrent_optimize_processes_percent</s:key>
                <s:key
name="path">splunkd.index_processor.index_optimization.concurrent_optimize_processes_percent</s:key>
            </s:dict>
        </s:key>
        <s:key name="display_name">Bucket Optimization</s:key>
        <s:key name="health">green</s:key>
        <s:key name="num_red">0</s:key>

```

```

        <s:key name="num_yellow">0</s:key>
      </s:dict>
    </s:key>
    <s:key name="num_red">0</s:key>
    <s:key name="num_yellow">0</s:key>
  </s:dict>
</s:key>
<s:key name="num_red">0</s:key>
<s:key name="num_yellow">0</s:key>
<s:key name="search_scheduler">
  <s:dict>
    <s:key name="health">green</s:key>
    <s:key name="num_red">0</s:key>
    <s:key name="num_yellow">0</s:key>
    <s:key name="search_lag">
      <s:dict>
        <s:key name="count_extremely_lagged_searches_last_hour">
          <s:dict>
            <s:key name="description"><![CDATA[This indicator checks whether there are any
extremely lagged searches in the last hour. These are scheduled searches which have been unable to run
within their configured interval. By default, this indicator is never Yellow, and is Red if there is at
least 1 extremely lagged scheduled search. This is a numeric threshold rather than a percentage. Setting
both thresholds to 0 will disable this indicator.]]></s:key>
            <s:key name="name">count_extremely_lagged_searches_last_hour</s:key>
          </s:dict>
        </s:key>
        <s:key name="display_name">Search Scheduler Search Lag</s:key>
        <s:key name="health">green</s:key>
        <s:key name="num_red">0</s:key>
        <s:key name="num_yellow">0</s:key>
        <s:key name="percent_searches_lagged_high_priority_last_24h">
          <s:dict>
            <s:key name="description"><![CDATA[This indicator tracks the lag rate of high
priority scheduled searches. Search lag is a delay that occurs before a search starts. High priority
scheduled searches are scheduled searches whose priority is set to "higher" or "highest". By default, this
indicator is yellow if the search lag rate exceeds 10%.]]></s:key>
            <s:key name="name">percent_searches_lagged_high_priority_last_24h</s:key>
          </s:dict>
        </s:key>
        <s:key name="percent_searches_lagged_non_high_priority_last_24h">
          <s:dict>
            <s:key name="description">This indicator tracks the lag rate for scheduled
searches whose priority is set to "default". Search lag is a delay that occurs before a search starts. By
default, this indicator is yellow if the search lag rate over the last 24 hours exceeds 40%.</s:key>
            <s:key name="name">percent_searches_lagged_non_high_priority_last_24h</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="searches_delayed">
      <s:dict>
        <s:key name="display_name">Search Scheduler Searches Delayed</s:key>
        <s:key name="health">green</s:key>
        <s:key name="num_red">0</s:key>
        <s:key name="num_yellow">0</s:key>
        <s:key name="percent_searches_delayed_high_priority_last_24h">

```

```

        <s:dict>
            <s:key name="description"><![CDATA[This indicator tracks the delayed search
rate for high priority scheduled searches. These are scheduled searches where the priority field is set to
"higher" or "highest". By default, this indicator is yellow if the delayed search ratio over the last 24
hours is 5%, and red if it is 10%.]]></s:key>
            <s:key name="name">percent_searches_delayed_high_priority_last_24h</s:key>
            <s:key
name="path">splunkd.search_scheduler.searches_delayed.percent_searches_delayed_high_priority_last_24h</s:key>
        </s:dict>
    </s:key>
    <s:key name="percent_searches_delayed_non_high_priority_last_24h">
        <s:dict>
            <s:key name="description">This indicator tracks the delayed search rate for
scheduled searches whose priority field is set to "default". By default, this indicator is yellow if the
delayed search ratio over the last 24 hours is 10%, and red if it is 20%.</s:key>
            <s:key name="name">percent_searches_delayed_non_high_priority_last_24h</s:key>
            <s:key
name="path">splunkd.search_scheduler.searches_delayed.percent_searches_delayed_non_high_priority_last_24h<
/s:key>
        </s:dict>
    </s:key>
    </s:dict>
    </s:key>
    </s:dict>
    <s:key name="searches_skipped">
        <s:dict>
            <s:key name="display_name">Search Scheduler Searches Skipped</s:key>
            <s:key name="health">green</s:key>
            <s:key name="num_red">0</s:key>
            <s:key name="num_yellow">0</s:key>
            <s:key name="percent_searches_skipped_high_priority_last_24h">
                <s:dict>
                    <s:key name="description"><![CDATA[This indicator tracks the skip rate for high
priority scheduled searches. These are scheduled searches where the priority field is set to "higher" or
"highest". By default, this indicator is yellow if the skipped search ratio over the last 24 hours is 5%,
and red if it is 10%.]]></s:key>
                    <s:key name="name">percent_searches_skipped_high_priority_last_24h</s:key>
                    <s:key
name="path">splunkd.search_scheduler.searches_skipped.percent_searches_skipped_high_priority_last_24h</s:key>
                </s:dict>
            </s:key>
            <s:key name="percent_searches_skipped_non_high_priority_last_24h">
                <s:dict>
                    <s:key name="description">This indicator tracks the skip rate for scheduled
searches whose priority field is set to "default". By default, this indicator is yellow if the skipped
search ratio over the last 24 hours is 10%, and red if it is 20%.</s:key>
                    <s:key name="name">percent_searches_skipped_non_high_priority_last_24h</s:key>
                    <s:key
name="path">splunkd.search_scheduler.searches_skipped.percent_searches_skipped_non_high_priority_last_24h<
/s:key>
                </s:dict>
            </s:key>
        </s:dict>
    </s:key>
    </s:dict>
    </s:dict>
    </s:key>
    </s:dict>
    </s:key>
    <s:key name="health">green</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
<i>health</i>	String	Indicates the overall health of <code>splunkd</code> . 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="b233a6clade2" 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
<i>health</i>	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.
<i>messages</i>	String	The last 50 messages from <code>splunkd.log</code> that might relate to the feature status change. Returned only if a feature color is not green.
<i>reasons</i>	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.
<i>due_to_stanza</i>	String	Indicates the stanza name in <code>health.conf</code> where the configuration for the non-green indicator exists.
<i>due_to_threshold</i>	String	Indicates the threshold because of which the color of the indicator is non-green.
<i>due_to_threshold_value</i>	Numeric	Indicates the value of the above threshold.
<i>indicator</i>	String	Name of the indicator because of which the feature is non-green.
<i>reason</i>	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="b233a6clade2" 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 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:dict>
  </content>
</entry>
```

```

        <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
<i>alert_action:&lt;action_name&gt;</i>	String	Specify the alert action name. <action_name> can be one of the following: [email   PagerDuty]
<i>action.to</i>	String	Primary email address to use with the email alert action.
<i>action.cc</i>	String	CC email address to use with the email alert action.

Name	Type	Description
<i>action.bcc</i>	String	BCC email address to use with the email alert action.
<i>action.integration_url_override</i>	String	Sets the <code>&lt;integration key&gt;</code> value for PagerDuty alert action. For example <code>action.integration_url_override=78c3b6cf0a884a538410fe2812273b0b</code>
<i>disabled</i>	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:passÂ https://localhost:8089/services/server/health-config/alert_action:emailÂ
-dÂ 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
<i>alert.disabled</i>	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).
<i>alert.min_duration_sec</i>	Number	The minimum amount of time, in seconds, that the health status color must persist before an alert triggers.
<i>alert.threshold_color</i>	String	The health status color that triggers an alert. Possible values are yellow and red. Default: red.
<i>alert:&lt;indicator_name&gt;.disabled</i>	Number	Possible values are 0 or 1. A value of 1 disables alerting for this indicator. Default: 0 (enabled).
<i>alert:&lt;indicator_name&gt;.min_duration_sec</i>	Number	The minimum amount of time, in seconds, that the health status color must persist before an alert triggers for this indicator.
<i>alert:&lt;indicator_name&gt;.threshold_color</i>	String	The health status color that triggers an alert for this indicator. Possible values are yellow and red. Default: red.
<i>disable</i>	Boolean	Disables/enables reporting the health of the feature. Use <code>disabled=1</code> to disable the feature. Use <code>disabled=0</code> to enable the feature.
<i>feature:&lt;feature_name&gt;</i>	String	Specify the feature name. <code>feature_name</code> can be any supported feature listed in <code>\$SPLUNK_HOME/etc/system/default/health.conf</code> .
<i>indicator:&lt;indicator name&gt;:&lt;color&gt;</i>	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="b233a6clade2" 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`

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
<i>activeLicenseGroup</i>	Type of Splunk software license. Enterprise Forwarder Free Invalid Trial
<i>addOns</i>	Names of active add-ons.
<i>build</i>	The build number for this Splunk instance version.
<i>cpu_arch</i>	The architecture type for the CPU hosting <code>splunkd</code> . The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.
<i>guid</i>	Globally unique identifier for this server.
<i>host</i>	Server name.
<i>host_fqdn</i>	<i>host</i> fully-qualified domain name.
<i>isFree</i>	Indicates if this server is running the Splunk instance under a free license.
<i>isTrial</i>	Indicates if this server is using a trial license.
<i>kv_store_status</i>	App KV store availability.
<i>license_labels</i>	Labels associated with the license used on this server.
<i>licenseKeys</i>	License key unique for each license.
<i>licenseSignature</i>	Hash signature for the license used on this server.
<i>licenseState</i>	Specifies the status of the license, which can be either OK or Expired.

Name	Description
<i>master_guid</i>	Globally unique identifier for this server.
<i>max_users</i>	Maximum number of users on the instance.
<i>mode</i>	Indicates whether the server is a dedicated forwarder. Possible values are: normal dedicated forwarder
<i>numberOfCores</i>	Server number of processor cores. The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.
<i>os_build</i>	Software build for the server <i>os_version</i> . The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.
<i>os_name</i>	Server operating system. The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.
<i>os_version</i>	Server operating system version. The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.
<i>physicalMemoryMB</i>	Server physical memory (MB). The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.
<i>product_type</i>	Splunk software product type. One of the following values. enterprise hunk lite lite_free splunk
<i>rtsearch_enabled</i>	Indicates if real-time search is enabled for the instance on this server.
<i>server_roles</i>	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: <code>server/roles</code> endpoint.
<i>serverName</i>	Server DNS domain name.
<i>startup_time</i>	Server platform start time, in seconds since January 1, 1970 (UNIX epoch).
<i>version</i>	<i>os_build</i> software version number. The value returned in the <code>server/info</code> response should be considered deprecated. Use <code>server/sysinfo</code> to access this response key and value instead.

### Example request and response



## XML Request

```
curl -k -u admin:changed https://10.140.53.114:8089/services/server/info
```

## XML Response

```
<title>server-info</title>
<id>https://localhost:8089/services/server/info</id>
<updated>2016-09-08T17:49:52-07:00</updated>
<generator build="19e4b5854495" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/info/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>server-info</title>
  <id>https://localhost:8089/services/server/info/server-info</id>
  <updated>2016-09-08T17:49:52-07:00</updated>
  <link href="/services/server/info/server-info" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/info/server-info" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="activeLicenseGroup">Trial</s:key>
      <s:key name="activeLicenseSubgroup">Production</s:key>
      <s:key name="addOns">
        <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="guid">C6AAF586-93E0-451B-914B-F63A8BBC7282</s:key>
                  <s:key name="maxNodes">200</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="build">19e4b5854495</s:key>
      <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">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:key name="guid">B4E173F1-034A-4D46-9DDC-ECF0016F165E</s:key>
<s:key name="host">docs-unix-4</s:key>
<s:key name="host_fqdn">docs-unix-4</s:key>
<s:key name="isForwarding">0</s:key>
<s:key name="isFree">0</s:key>
<s:key name="isTrial">1</s:key>
<s:key name="kvStoreStatus">ready</s:key>
<s:key name="licenseKeys">
  <s:list>
    <s:item>6D234F85995D32F1830F3123AF3826FCC7F0B3DF7CFE460562773A3ECD08DA51</s:item>
  </s:list>
</s:key>
<s:key name="licenseSignature">81239ffa950c89dde6de2970bb25438c4</s:key>
<s:key name="licenseState">OK</s:key>
<s:key name="license_labels">
  <s:list>
    <s:item>Splunk Enterprise + Hunk Download Trial</s:item>
  </s:list>
</s:key>
<s:key name="master_guid">B4E234F1-02AA-4D46-9DDC-ECF0016F165E</s:key>
<s:key name="max_users">4294967295</s:key>
<s:key name="mode">normal</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="product_type">enterprise</s:key>
<s:key name="rtsearch_enabled">1</s:key>
<s:key name="serverName">docs-unix-4</s:key>
<s:key name="server_roles">
  <s:list>
    <s:item>indexer</s:item>
    <s:item>license_master</s:item>
    <s:item>kv_store</s:item>
  </s:list>
</s:key>
<s:key name="startup_time">1473344210</s:key>
<s:key name="staticAssetId">630EA7F9747711232091234BF3B6F9916315C2C368C8D61EF4B986BE1F28E7E0</s:key>
<s:key name="version">6.5.0</s:key>
</s:dict>
</content>
</entry>

```

## 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. <ul style="list-style-type: none"><li>• normal</li><li>• throttled</li><li>• stopped</li></ul>

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	<div>Returns the following JSON document.</div> <div><ul style="list-style-type: none"><li>• count - Number of collection documents or objects.</li><li>• indexSizes - Key and size of every index on the collection.</li><li>• lastExtentSize - Size of last allocated extent.</li><li>• nindexes - Number of indexes on the collection.</li><li>• ns - Current collection namespace.</li><li>• numExtents - Number of contiguously allocated data file regions.</li><li>• paddingFactor - Amount of space added to each document.</li><li>• size - Collection records total size.</li><li>• storageSize- Collection document storage allocation.</li><li>• systemFlags - Collection flags that reflect internal server options.</li><li>• totalIndexSize - Size of all indexes.</li><li>• userFlags - Collection flags set by user.</li></ul></div> <div>Note: Sizes are returned in MBs. For more information, see Performance Metrics.</div>

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
<i>data</i>	Returns the following CDATA items. <ul style="list-style-type: none"><li>• asserts - Number of database assertions since the server process started, for each of the following levels/types:<ul style="list-style-type: none"><li>◆ regular</li><li>◆ warning</li><li>◆ msg</li><li>◆ user</li><li>◆ rollovers</li></ul></li><li>• backgroundFlushing - Write to disk flush metrics:<ul style="list-style-type: none"><li>◆ flushes - Number of times writes flushed.</li><li>◆ total_ms - Number of msec processes used to flush writes.</li><li>◆ average_ms - Relationship between flushes and total_ms, in msec.</li><li>◆ last_ms - Number of msec the last flush took.</li><li>◆ last_finished (date) - ISO time of last completed write flush operation.</li></ul></li><li>• connections - Current incoming connections status and database availability:<ul style="list-style-type: none"><li>◆ current - Number of active client connections.</li><li>◆ available - Number of unused connections available.</li></ul></li></ul>

Name	Description
	<ul style="list-style-type: none"> <li>♦ <code>totalCreated</code> - Total number of connections created, including closed connections.</li> <li>• <code>cursors</code> - [DEPRECATED] Current cursor and state. Use <code>metrics</code>, instead.</li> <li>• <code>dur</code> - (Durability) Journaling-related operations and performance. Journaling must be enabled.: <ul style="list-style-type: none"> <li>♦ <code>commits</code> - Number of transactions written to the journal during the last group commit interval.</li> <li>♦ <code>journalizedMB</code> - Amount of data (MB) written to the journal during the last group commit interval.</li> <li>♦ <code>writeToDataFilesMB</code> - Amount of data (MB) written from journal to data files during the last group commit interval.</li> <li>♦ <code>compression</code> - Compression ratio of data written to journal: (<code>journalized_size_of_data</code> / <code>uncompressed_size_of_data</code>)</li> <li>♦ <code>commitsInWriteLock</code> - Number of commits that occurred during a write lock.</li> <li>♦ <code>earlyCommits</code> - Number of commits requested before scheduled group commit time.</li> <li>♦ <code>timeMs</code>: Performance during various journaling phases. <ul style="list-style-type: none"> <li>♦ <code>dt</code> - Data collection interval (msec).</li> <li>♦ <code>prepLogBuffer</code> - Time spend preparing to write to journal (msec).</li> <li>♦ <code>writeToJournal</code> - Time spent writing to journal (msec).</li> <li>♦ <code>writeToDataFiles</code> - Time spent writing to data files after journaling (msec).</li> <li>♦ <code>remapPrivateView</code> - Time spent remapping copy-on-write memory mapped views (msec).</li> </ul> </li> </ul> </li> <li>• <code>extra_info</code> - Platform-specific information: <ul style="list-style-type: none"> <li>♦ <code>note</code> - Platform-specific information.</li> <li>♦ <code>heap_usage_bytes</code> - Total heap space size used by database (bytes). Applicable to *nix systems, only.</li> <li>♦ <code>page_faults</code> - Total number of page faults that require disk operations.</li> </ul> </li> <li>• <code>globalLock</code> - Information about the current database lock state, historical lock status, and active clients: <ul style="list-style-type: none"> <li>♦ <code>totalTime</code> - Time since database started and <code>globalLock</code> creation (usec).</li> <li>♦ <code>lockTime</code> - Time since database started that <code>globalLock</code> has been held (usec).</li> <li>♦ <code>currentQueue</code>: Information about operations queued because of a lock. <ul style="list-style-type: none"> <li>♦ <code>total</code> - Total number of operations queued waiting on <code>readers</code> and <code>writers</code> locks.</li> <li>♦ <code>readers</code> - Number of operations queued waiting for read lock.</li> <li>♦ <code>writers</code> - Number of operations queued waiting for write lock.</li> </ul> </li> <li>♦ <code>activeClients</code>: Information about number and operation types of connected clients. <ul style="list-style-type: none"> <li>♦ <code>total</code> - Total number of <code>readers</code> and <code>writers</code> connections.</li> <li>♦ <code>readers</code> - Number of connected clients performing read operations.</li> <li>♦ <code>writers</code> - Number of connected clients performing write operations.</li> </ul> </li> </ul> </li> <li>• <code>host</code> - Hostname and port number.</li> <li>• <code>indexCounters</code> - Index usage counters: <ul style="list-style-type: none"> <li>♦ <code>accesses</code> - Number of times operations accessed indexes.</li> <li>♦ <code>hits</code> - Number of times index accessed and returned from memory.</li> <li>♦ <code>misses</code> - Number of attempts to access index not in memory.</li> <li>♦ <code>resets</code> - Number of times index counters reset since database last started.</li> <li>♦ <code>missRatio</code> - Ratio of hits to misses.</li> </ul> </li> <li>• <code>localTime</code> - ISO-formatted local time.</li> <li>• <code>locks</code> - State and read/write use of global and database-specific locks: <ul style="list-style-type: none"> <li>♦ <code>timeLockedMicros</code> - Amount of time a lock existed, for all databases of this server instance (usec).</li> <li>♦ <code>timeAcquiringMicros</code> - Amount of time operations spend waiting, for lock for all databases of this server instance (usec).</li> <li>♦ <code>admin</code>: Lock use in the admin database. <ul style="list-style-type: none"> <li>♦ <code>timeLockedMicros</code> - Amount of time locks existed in the admin database context (usec).</li> <li>♦ <code>timeAcquiringMicros</code> - Amount of time spent waiting to acquire a lock in the admin database context (usec).</li> </ul> </li> <li>♦ <code>local</code>: Lock use in the local database. <ul style="list-style-type: none"> <li>♦ <code>timeLockedMicros</code> - Amount of time locks existed in the local database context (usec).</li> <li>♦ <code>timeAcquiringMicros</code> - Amount of time spent waiting to acquire a lock in the local database context (usec).</li> </ul> </li> <li>♦ <code>search.&lt;collection&gt;</code>: Locks used in each collection. <ul style="list-style-type: none"> <li>♦ <code>timeLockedMicros</code> - Amount of time locks exist in the collection context (usec).</li> <li>♦ <code>timeAcquiringMicros</code> - Amount of time spent waiting to acquire a lock in the collection context (usec).</li> </ul> </li> </ul> </li> <li>• <code>mem</code> - Memory usage: System architecture and memory usage metrics. <ul style="list-style-type: none"> <li>♦ <code>bits</code> - System address architecture: 32 or 64 bit architecture.</li> <li>♦ <code>resident</code> - Amount of RAM currently used by the database process (MB).</li> </ul> </li> </ul>

Name	Description
	<ul style="list-style-type: none"> <li>◆ <b>virtual</b> - Amount of virtual memroy used (MB).</li> <li>◆ <b>supported: true</b> = supports extended memory information, <b>false</b> = does not support extended memory information.</li> <li>◆ <b>mapped</b> - Amount of mapped memory for database (MB).</li> <li>◆ <b>mappedWithJournal</b> - Amount of mapped memory, including journaling memory (MB). Always twice the size of mapped.</li> <li>• <b>metrics</b> - Current instance use and state: <ul style="list-style-type: none"> <li>◆ <b>cursor</b>: Cursor state and use. <ul style="list-style-type: none"> <li>◇ <b>timedOut</b> - Total number of cursors that have timed out since the server process started.</li> <li>◇ <b>open</b>: - Information about open cursors. <ul style="list-style-type: none"> <li>· <b>noTimeout</b> - Number of open cursors with option set to prevent timeout after a period of inactivity.</li> <li>· <b>pinned</b> - Number of pinned open cursors.</li> <li>· <b>total</b> - Number of cursors maintained for clients, typically less than zero.</li> </ul> </li> </ul> </li> <li>◆ <b>document</b>: Information about document access and modification patterns and data use. Compare these values to <b>opcounters data</b>, which track total number of operations. <ul style="list-style-type: none"> <li>◇ <b>deleted</b> - Total number of deleted documents.</li> <li>◇ <b>inserted</b> - Total number of inserted documents.</li> <li>◇ <b>returned</b> - Total number of documents returned by queries.</li> <li>◇ <b>updated</b> - Total number of updated documents.</li> </ul> </li> <li>◆ <b>getLastError</b>: Information about <b>getLastError</b> use. <ul style="list-style-type: none"> <li>◇ <b>wtime</b>: <b>getLastError</b> operation counts with a specified write concern that wait for one or more members of a replica set to acknowledge the write operation. <ul style="list-style-type: none"> <li>· <b>num</b> - <b>getLastError</b> operation counts with a specified write concern that wait for one or more members of a replica set to acknowledge the write operation.</li> <li>· <b>totalMillis</b> - Amount of time spent performing <b>getLastError</b> operations with write concern that wait for one or more members of a replica set to acknowledge the write operation (msec).</li> </ul> </li> <li>◇ <b>wtimeouts</b> - Number of times write concern operations timed out as a result of the <b>wtimeout</b> threshold to <b>getLastError</b>.</li> </ul> </li> <li>◆ <b>operation</b>: Counters for several types of update and query operations handled using special operation types. <ul style="list-style-type: none"> <li>◇ <b>fastmod</b> - Number of update operations that neither cause documents to grow nor require updates to the index.</li> <li>◇ <b>idhack</b> - Number of queries that contain the <b>_key</b> field.</li> <li>◇ <b>scanAndOrder</b> - Number of queries that return sorted numbers that cannot perform the sort operation using an index.</li> </ul> </li> <li>◆ <b>queryExecutor</b>: Data from the query execution system. <ul style="list-style-type: none"> <li>◇ <b>scanned</b> - Number of index items scanned during queries and query-plan evaluation.</li> <li>◇ <b>scannedObjects</b> - Total number of documents scanned during the query.</li> </ul> </li> <li>◆ <b>record</b>: Data related to record allocation in the on-disk memory files. <ul style="list-style-type: none"> <li>◇ <b>moves</b> - 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.</li> </ul> </li> <li>◆ <b>repl</b>: Metrics related to the ordered history of logical writes. <ul style="list-style-type: none"> <li>◇ <b>apply</b>: - Information about the application of ordered history of logical writes. <ul style="list-style-type: none"> <li>· <b>batches</b>: Information on the ordered history of logical writes application process on secondaries members of replica sets. <ul style="list-style-type: none"> <li>• <b>num</b> - Number of batches applied across all databases.</li> <li>• <b>totalMillis</b> - Amount of time spent applying ordered history of logical write operations (msec).</li> </ul> </li> <li>· <b>ops</b> - Number of ordered history of logical write operations.</li> </ul> </li> <li>◇ <b>buffer</b>: Information to track the ordered history of logical write operations buffer. <ul style="list-style-type: none"> <li>· <b>count</b> - Number of operations on the ordered history of logical writes buffer.</li> <li>· <b>maxSizeBytes</b> / - Maximum size of the ordered history of logical writes buffer.</li> <li>· <b>sizeBytes</b> - Current size of the contents of the ordered history of logical writes buffer.</li> </ul> </li> <li>◇ <b>network</b>: Network use information for the replication process. <ul style="list-style-type: none"> <li>· <b>bytes</b> - Amount of data read from the replication sync source (bytes).</li> <li>· <b>getmores</b>: Information about queries for additional results from the ordered history of logical write operations cursor as part of the replication process.</li> </ul> </li> </ul> </li> </ul> </li> </ul>

Name	Description
	<ul style="list-style-type: none"> <li>• <b>num</b> - 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.</li> <li>• <b>totalMillis</b> - Amount of time to collect data from queries for additional results from the ordered history of logical write operations (msec).</li> <li>• <b>ops</b> - Number of operations read from the replication source.</li> <li>• <b>readersCreated</b> - Number of queries for additional results from the ordered history of logical write operations processes created.</li> <li>◊ <b>preload</b>: Information about replication pre-fetch. <ul style="list-style-type: none"> <li>• <b>docs</b>: Information about documents loaded into memory during replication pre-fetch. <ul style="list-style-type: none"> <li>• <b>num</b> - Number of documents loaded during replication pre-fetch.</li> <li>• <b>totalMillis</b> - Amount of time spent loading documents as part of replication pre-fetch (msec).</li> </ul> </li> <li>• <b>indexes</b>: Information about index items loaded into memory during replication pre-fetch. <ul style="list-style-type: none"> <li>• <b>num</b> - Number of index entries loaded by members before updating documents as part of replication pre-fetch.</li> <li>• <b>totalMillis</b> - Amount of time spent loading index entries as part of replication pre-fetch (msec).</li> </ul> </li> </ul> </li> <li>◊ <b>storage</b>: Freelist behavior monitoring statistics. <ul style="list-style-type: none"> <li>◊ <b>freelist</b>: Freelist bucket behavior monitoring statistics. <ul style="list-style-type: none"> <li>• <b>search</b>: Freelist bucket behavior monitoring search statistics. <ul style="list-style-type: none"> <li>• <b>bucketExhausted</b> - Number of times bucket fully searched, requiring advance to next bucket.</li> <li>• <b>requests</b> - Number of times the allocation function was called.</li> <li>• <b>scanned</b> - Number of freelist bucket entries examined.</li> </ul> </li> </ul> </li> </ul> </li> <li>◊ <b>ttl</b>: Information about resource use of the ttl index process. <ul style="list-style-type: none"> <li>◊ <b>deletedDocuments</b> - Number of documents deleted from collections with a ttl index.</li> <li>◊ <b>passes</b> - Number of times background process removes documents from collections with a ttl index.</li> </ul> </li> <li>• <b>network</b> - Network use and state: <ul style="list-style-type: none"> <li>◊ <b>bytesIn</b> - Amount of network traffic received by this database (bytes).</li> <li>◊ <b>bytesOut</b> - Amount of network traffic sent from this database (bytes).</li> <li>◊ <b>numRequests</b> - Number of distinct requests received by the server.</li> </ul> </li> <li>• <b>ok</b> - Command return status: 1 = Success, 0 = Failure.</li> <li>• <b>opcounters</b> - Overview of database operations by type, similar to <b>opcountersRepl</b>: <ul style="list-style-type: none"> <li>◊ <b>insert</b> - Number of insert operations since instance started.</li> <li>◊ <b>query</b> - Number of queries since instance started.</li> <li>◊ <b>update</b> - Number of update operations since instance started.</li> <li>◊ <b>delete</b> - Number of delete operations since instance started.</li> <li>◊ <b>getmore</b> - Number of <b>getmore</b> operations since instance started.</li> <li>◊ <b>command</b> - Number of commands issued since instance started.</li> </ul> </li> <li>• <b>opcountersRepl</b> - Overview of replication operations by type, similar to <b>opcounters</b>: <ul style="list-style-type: none"> <li>◊ <b>insert</b> - Number of replicated insert operations since instance started.</li> <li>◊ <b>query</b> - Number of replicated queries since instance started.</li> <li>◊ <b>update</b> - Number of replicated update operations since instance started.</li> <li>◊ <b>delete</b> - Number of replicated delete operations since instance started.</li> <li>◊ <b>getmore</b> - Number of replicated <b>getmore</b> operations since instance started.</li> <li>◊ <b>command</b> - Number of replicated commands issued since instance started.</li> </ul> </li> <li>• <b>pid</b> - Process ID.</li> <li>• <b>recordStats</b> - Page fault statistics: <ul style="list-style-type: none"> <li>◊ <b>accessesNotInMemory</b> - Number of times memory page accessed that was not resident in memory, for all databases.</li> <li>◊ <b>pageFaultExceptionsThrown</b> - Number of page fault exceptions thrown when accessing data for all databases.</li> <li>◊ <b>admin</b>: Admin database page fault statistics. <ul style="list-style-type: none"> <li>◊ <b>accessesNotInMemory</b> - Number of times memory page accessed that was not resident in memory, for the admin database.</li> <li>◊ <b>pageFaultExceptionsThrown</b> - Number of page fault exceptions thrown when accessing data for the admin database.</li> </ul> </li> <li>◊ <b>local</b>: Local database page fault statistics.</li> </ul> </li> </ul>



Name	Description
	<ul style="list-style-type: none"> <li>◊ <code>accessesNotInMemory</code> - Number of times memory page accessed that was not resident in memory, for the local database.</li> <li>◊ <code>pageFaultExceptionsThrown</code> - Number of page fault exceptions thrown when accessing data for the local database.</li> <li>◆ <code>search.&lt;collection&gt;</code>: Search database page fault statistics. <ul style="list-style-type: none"> <li>◊ <code>accessesNotInMemory</code> - Number of times memory page accessed that was not resident in memory, for the search database.</li> <li>◊ <code>pageFaultExceptionsThrown</code> - Number of page fault exceptions thrown when accessing data for the search database.</li> </ul> </li> <li>• <code>uptime</code> - Amount of time database process has been active (seconds).</li> <li>• <code>uptimeEstimate</code> - Amount of time database process has been active as calculated from the internal, course-grained time keeping system (seconds).</li> <li>• <code>uptimeMillis</code> - Amount of time database process has been active (msec).</li> <li>• <code>version</code> - Version number (not used).</li> <li>• <code>writeBacksQueued</code> - Write-backs queued status: <code>true</code> = write-backs queued, <code>false</code> = write-backs not queued.</li> </ul>

## 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, "journalMB":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
<i>Bundle_Directory_Reaper_Average_Time(ms)</i>	Average time for dispatch reaper to walk search peer directory and reap obsolete bundles.
<i>Bundle_Directory_Reaper_Max_Time(ms)</i>	Maximum time for dispatch reaper to walk search peer directory and reap obsolete bundles.
<i>Compute_User_Search_Quota_Average_Time(ms)</i>	Average time for computing user search quota.
<i>Compute_User_Search_Quota_Max_Time(ms)</i>	Maximum time for computing user search quota.
<i>Dispatch_Directory_Reaper_Average_Time(ms)</i>	Average time for dispatch reaper to walk dispatch directory and reap stale artifacts.
<i>Dispatch_Directory_Reaper_Max_Time(ms)</i>	Maximum time for dispatch reaper to walk dispatch directory and reap stale artifacts.
<i>Search_StartUp_Time_Average_Time(ms)</i>	Average time for preprocessing before search startup. Counted from time search state is set to <code>RUNNING</code> .

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.
<i>Search_StartUp_Time_Max_Time(ms)</i>	<p>Maximum time for preprocessing before search startup. Counted from time search state is set to <code>RUNNING</code>.</p> <p>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.</p>

## 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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

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

```

```

    <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
<i>Bundle_Directory_Reaper_Average_Time(ms)</i>	Average time for dispatch reaper to walk search peer directory and reap obsolete bundles.
<i>Bundle_Directory_Reaper_Max_Time(ms)</i>	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>

```

```
</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](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
<i>Dispatch_Directory_Reaper_Average_Time(ms)</i>	Average time for dispatch reaper to walk dispatch directory and reap stale artifacts.
<i>Dispatch_Directory_Reaper_Max_Time(ms)</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
```

```

<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](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
<i>Search_StartUp_Time_Average_Time(ms)</i>	Average time for preprocessing before search startup. Counted from time search state is set to RUNNING.
<i>Search_StartUp_Time_Max_Time(ms)</i>	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
<i>Get_Authentication_Max_Time(ms)</i>	Maximum time for search head to get authentication from this peer.
<i>Get_Authentication_Mean_Time(ms)</i>	Average time for search head to get authentication from this peer.
<i>Get_BundleList_Max_Time(ms)</i>	Maximum time for search head to get bundle list from this peer.
<i>Get_ServerInfo_Max_Time(ms)</i>	Maximum time for search head to get server information back from this peer.
<i>Get_ServerInfo_Mean_Time(ms)</i>	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
<i>final_score</i>	Most recent calculated priority score, based on adjustments and original score.



Name	Description
<i>name</i>	Scheduled search name.
<i>orig_score</i>	A score based on a search's originally scheduled run time.
<i>owner</i>	Search scope or context owner. This could be a specific user or "nobody" for a search defined in an app or system-level scope.
<i>priority_no</i>	Most recent calculated priority number for this search.
<i>real_time_adj</i>	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.
<i>runtime_adj</i>	Calculated value based on average search runtime.
<i>skipped_adj</i>	Adjustment for number of times search has been skipped and search period. 0 means the search has not been skipped.
<i>window_adj</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

        </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
<i>count_realtime</i>	Jobs active in the immediate past observation period, not including historical jobs.
<i>count_scheduled</i>	Jobs active in the immediate past observation period, not including real-time jobs.
<i>count_summary</i>	Jobs active in the immediate past observation period, not including non-summary jobs.
<i>top_apps</i>	Top 15 apps in the past observation period, in <i>app:count</i> key-value pair format.
<i>top_named_searches</i>	Top 15 named searches in the past observation period, in <i>savedSearchName:count</i> key-value pair format.
<i>top_users</i>	Top 15 users in the past observation period, in <i>username:count</i> key-value pair format, with <i>count</i> as the number of app contexts for the user.
<i>total_count</i>	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
<i>key_count</i>	Number of file input records (keys) seen since start-up.
<i>total_size</i>	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
<i>refresh</i>	Boolean	Set to <code>true</code> to perform a new file integrity check. Only one such check can be performed at a time.
<i>regex_filter</i>	PCRE regular expression	Specify a regular expression to filter results of the check. For example, use <code>regex_filter=\.conf\$</code> 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.
<i>access_failed</i>	The <code>splunkd</code> process does not have permissions to read the file.
<i>differs</i>	The installed file differs from the manifest file.
<i>missing</i>	The installed file was not found.
<i>read_failed</i>	The installed file comparison failed.
<i>other_open_failed</i>	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
<i>max_auto_summary_searches</i>	Maximum number of auto summary searches.
<i>max_hist_scheduled_searches</i>	Maximum number of historical scheduled searches.
<i>max_hist_searches</i>	Maximum number of historical searches.
<i>max_rt_scheduled_searches</i>	Maximum number of scheduled searches.
<i>max_rt_searches</i>	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
<i>capacity</i>	Disk capacity (MB).

Name	Description
<i>free</i>	Disk free space (MB).
<i>fs_type</i>	File system type. Example values: <ul style="list-style-type: none"> <li>• Linux: ext2, ext3, ext4, qnx4</li> <li>• Solaris: ufs, zfs</li> <li>• Windows: ntfs, fat32</li> <li>• AIX: jfs</li> <li>• (not OS-specific) WORM: ISO9660, UDF13346</li> <li>• (not OS-specific); network-shared: SMB, CIFS, NFS</li> <li>• (not OS-specific) Veritas: VxFS.</li> </ul>
<i>mount_point</i>	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
<i>cpu_arch</i>	CPU architecture
<i>cpu_count</i>	CPU count
<i>cpu_idle_pct</i>	Percentage of time CPU is idle. Value reported as 100.0 on Windows except for Vista+ and XP/Win2003 English-only operating systems.

Name	Description
<i>cpu_system_pct</i>	Percentage of time CPU is running in system mode. Missing from Windows except for Vista+ and XP/Win2003 English-only operating systems.
<i>cpu_user_pct</i>	Percentage of time CPU is running in user mode. Missing from Windows except for Vista+ and XP/Win2003 English-only operating systems.
<i>forks</i>	Cumulative number of forked processes since OS startup. Not available on Windows.
<i>mem</i>	Total physical memory available (MB)
<i>mem_used</i>	<p>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.</p> <p>On Unix, <i>mem_used</i> = <code>total_phys_ram - (free_mem + buffer_mem + cached_mem + slab_reclaimable)</code>  On Windows, <i>mem_used</i> = <code>(memoryStatus.ullTotalPhys - memoryStatus.ullAvailPhys)</code> See <code>GlobalMemoryStatusEx</code> function for more information.</p>
<i>normalized_load_avg_1min</i>	Normalized load average of <i>runnable_process_count</i> across all cores ( <code>cumulative_load_avg / number_of_cores</code> ). This value is not reliable for a VM guest.
<i>os_build</i>	Software build for the <i>os_version</i>
<i>os_name</i>	Operating system name
<i>os_name_ext</i>	Extended operating system name
<i>os_version</i>	Operating system version
<i>pg_paged_out</i>	Cumulative VM page count paged since OS startup. Not available on Windows.
<i>pg_swapped_out</i>	Cumulative pages swapped out since OS startup. Not available on Windows.
<i>runnable_process_count</i>	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.
<i>splunk_version</i>	Currently installed Splunk software version
<i>swap</i>	Amount of disk allocated to swap (fractional MB)
<i>swap_used</i>	Swap space currently in use (fractional MB)
<i>virtual_cpu_count</i>	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:dict>
  </content>
</entry>

```

```
<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
<i>avg_service_ms</i>	Average time requests caused the CPU to be in use, in milliseconds.
<i>avg_total_ms</i>	Average queue + execution time for requests to be completed, in milliseconds.
<i>cpu_pct</i>	Percentage of time the CPU was servicing requests.
<i>device</i>	Device name (e.g., as listed under /dev on UNIX).
<i>fs_type</i>	Mounted device file system type.
<i>interval</i>	Interval over which sampling occurred, in seconds.
<i>mount_point</i>	Mount point(s) of the underlying device.
<i>reads_kb_ps</i>	Total number of kb read per second.
<i>reads_ps</i>	Number of read requests per second.
<i>writes_kb_ps</i>	Total number of kb written per second.
<i>writes_ps</i>	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
<i>args</i>	Non-search process arguments.
<i>cpu_system_time</i>	Cumulative time this process has spent executing in kernel (incl. system calls). Extra field.
<i>cpu_user_time</i>	Cumulative time this process has spent executing in user space (incl. library functions). Extra field.
<i>elapsed</i>	Elapsed wall time, accurate to within the collection period.
<i>fd_used</i>	Number of currently open files used by this process.
<i>label</i>	Human-readable label for the saved search.
<i>mem_unshared_data_used</i>	Amount of heap and stack used. Not available on Windows. Extra field.
<i>mem_used</i>	Current amount of resident physical memory used (KB). (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, <i>mem_used</i> is obtained by reading the <code>WorkingSetSize</code> property returned by the <code>GetProcessMemoryInfo()</code> function (see <code>GetProcessMemoryInfo</code> function and <code>PROCESS_MEMORY_COUNTERS</code> structure).
<i>normalized_pct_cpu</i>	Percentage of CPU usage across all cores. 100% is equivalent to all CPU resources on the machine.
<i>page_faults</i>	Number of major page faults. Extra field.
<i>pct_cpu</i>	Percentage of CPU usage, relative to one core. 100% is equivalent to 1 core.

Name	Description
<i>pct_memory</i>	Percentage of physical memory used hostwide (( <i>mem_used</i> /available_host_memory) * 100).
<i>pid</i>	Process ID.
<i>ppid</i>	Parent process ID. Not available for all processes.
<i>process</i>	Process name. The .exe suffix is stripped on Windows operating systems.
<i>read_mb</i>	Amount of data read (MB), excluding cache reads.
<i>search_head</i>	Dispatching search head for processes running saved searches.
<i>search_props</i>	<p>Search properties map of the following key value pairs.</p> <ul style="list-style-type: none"> <li>• <b>acceleration_id</b>: Acceleration ID</li> <li>• <b>app</b>: App name</li> <li>• <b>mode</b>: One of the following search modes. <ul style="list-style-type: none"> <li>◆ historical</li> <li>◆ historical batch</li> <li>◆ RT</li> <li>◆ RT indexed</li> </ul> </li> <li>• <b>provenance</b>: One of the following search sources. <ul style="list-style-type: none"> <li>◆ cli</li> <li>◆ rest</li> <li>◆ ui:&lt;App&gt;:&lt;View&gt;</li> </ul> </li> <li>• <b>role</b>: Splunk Enterprise platform role. Either head or peer.</li> <li>• <b>scan_count</b>: 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.</li> <li>• <b>delta_scan_count</b>: 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.</li> <li>• <b>sid</b>: Search ID (SID).</li> <li>• <b>type</b>: One of the following search types. <ul style="list-style-type: none"> <li>◆ ad-hoc</li> <li>◆ datamodel acceleration</li> <li>◆ other</li> <li>◆ report acceleration</li> <li>◆ scheduled</li> <li>◆ summary indexing</li> </ul> </li> <li>• <b>user</b>: Splunk username who initiated the search</li> </ul>
<i>status</i>	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.
<i>t_count</i>	Current number of threads.
<i>written_mb</i>	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
<code>cpu_arch</code>	Server CPU architecture.
<code>numberOfCores</code>	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 <code>splunkd.log</code> .
<code>numberOfVirtualCores</code>	Number of server virtual cores.
<code>os_build</code>	Software build for the server <code>os_version</code> .
<code>os_name</code>	Server operating system name.
<code>os_name_extended</code>	Server operating system name.
<code>os_version</code>	Server operating system version.
<code>physicalMemoryMB</code>	Server physical memory (MB). The same value is returned as the <code>mem</code> field from <code>server/status/resource-usage/hostwide</code> . A value of 0 is returned if the number cannot be accessed and the access failure reason is logged to <code>splunkd.log</code> .
<code>transparent_hugepages</code>	<p>For Linux systems, includes the following THP status indicators.</p> <ul style="list-style-type: none"><li>• <code>defrag</code></li><li>• <code>effective_state</code></li><li>• <code>enabled</code></li></ul> <p>For non-Linux systems, <code>effective_state</code> is set to <code>ok</code></p>
<code>ulimits</code>	<p>On all UNIX systems, lists settings for the following <code>ulimits</code> in place on <code>splunkd</code> at runtime.</p> <ul style="list-style-type: none"><li>• <code>core_file_size</code></li><li>• <code>cpu_time</code></li><li>• <code>data_file_size</code></li><li>• <code>data_segment_size</code></li><li>• <code>nice</code></li><li>• <code>open_files</code></li><li>• <code>resident_memory_size</code></li><li>• <code>stack_size</code></li><li>• <code>user_processes</code></li></ul>

Name	Description
	• 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:dict>
  </content>
</entry>
</s:messages>
```

```

    </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](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
<i>count</i>	Number	Number of bookmark URLs to list.
<i>offset</i>	Number	Lists bookmark URLs, offset from the first bookmark.

Name	Type	Description
<i>search</i>	String	Items to search for, must be valid as SPL.
<i>sort_dir</i>	Enum	asc or desc; ascending or descending
<i>sort_key</i>	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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```



```

        <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
<i>name</i>	String	Name of the deployment bookmark.
<i>url</i>	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 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.

## 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
<i>search</i>	The data models, represented as search strings.
<i>summary.access_count</i>	The total number of times that the summary for each data model has been accessed.
<i>summary.access_time</i>	The last time that the summary of each data model was accessed.
<i>summary.average_time</i>	The average runtime of the past 48 summarization search jobs for this data model.
<i>summary.buckets</i>	The total number of buckets in the summaries of each data model.
<i>summary.buckets_size</i>	The total size of the buckets in the summaries of each data model. The size is reported in terms of megabytes (MB).
<i>summary.complete</i>	Reports whether or not the summaries for each data model are complete.
<i>summary.earliest_time</i>	The timestamp of the earliest event in the summaries for each data model.
<i>summary.id</i>	The ID of the data models being summarized. The format is <code>DM_&lt;app_name&gt;_&lt;data_model_ID&gt;</code> .
<i>summary.is_inprogress</i>	Indicates whether or not the summary build is currently in progress for each data model.
<i>summary.last_error</i>	Lists errors that were logged in the latest run (from <code>last_sid</code> ) of the summary creation search.
<i>summary.last_sid</i>	The SID of the latest creation search job for each data model summary.
<i>summary.latest_time</i>	The timestamp of the latest events in each data model summary.
<i>summary.latest_dispatch_time</i>	The timestamp of the latest summary creation search for each data model.
<i>summary.latest_run_duration</i>	The runtime of the latest summary creation search for each data model.
<i>summary.mod_time</i>	The last time each data model summary was modified.
<i>summary.p50</i>	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.
<i>summary.p90</i>	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.
<i>summary.run_stats</i>	The start and duration of all saved previous summarization search jobs, up to 100 jobs.

Name	Description
<i>summary.size</i>	The total size of each summary, in bytes.
<i>summary.time_range</i>	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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```



```

        <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
------	------	---------	-------------

<i>app</i> required	string		The short name of the app to which this data set belongs.
<i>data model ID</i> required	string		The ID of the data model.

## Returned values

Name	Description
<i>search</i>	The data model, represented as a search string.
<i>summary.access_count</i>	The total number of times that the summary for this data model has been accessed.
<i>summary.access_time</i>	The last time that the summary of this data model was accessed.
<i>summary.average_time</i>	The average runtime of the past 48 summarization search jobs for this data model.
<i>summary.buckets</i>	The total number of buckets in the summary of this data model.
<i>summary.buckets_size</i>	The total size of the buckets in the summary of this data model. The size is reported in terms of megabytes (MB).
<i>summary.complete</i>	Reports whether or not the summary for the data model are complete.
<i>summary.earliest_time</i>	The timestamp of the earliest event in the summary for this data model.
<i>summary.id</i>	The ID of the data model being summarized. The format is DM_<app_name>_<data_model_ID>.
<i>summary.is_inprogress</i>	Indicates whether or not the data model summary build is currently in progress.
<i>summary.last_error</i>	Lists errors that were logged in the latest run (from <i>last_sid</i> ) of the summary creation search.
<i>summary.last_sid</i>	The SID of the latest data model summary creation search job.
<i>summary.latest_time</i>	The timestamp of the latest event in the data model summary.
<i>summary.latest_dispatch_time</i>	The timestamp of the latest summary creation search for the data model.
<i>summary.latest_run_duration</i>	The runtime of the latest summary creation search for the data model.
<i>summary.mod_time</i>	The last time the data model summary was modified.
<i>summary.p50</i>	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.
<i>summary.p90</i>	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.
<i>summary.run_stats</i>	The start and duration of all saved previous summarization search jobs, up to 100 jobs.
<i>summary.size</i>	The total size of the summary, in bytes.
<i>summary.time_range</i>	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.

GET

List lookup table files.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

Name	Description
<i>eai:appName</i>	The app for which the lookup table applies.
<i>eai:data</i>	The source path for the lookup staging area. The lookup table file is moved from here into \$SPLUNK_HOME.
<i>eai:userName</i>	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
<i>eai:data</i> 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.
<i>name</i> required	String		The lookup table filename.

### Returned values

Name	Description
<i>eai:appName</i>	The app for which the lookup table applies.
<i>eai:data</i>	The source path for the lookup staging area. The lookup table file is moved from here into \$SPLUNK_HOME.
<i>eai:userName</i>	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 -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.

## 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
------	-------------



<i>eai:appName</i>	The app for which the lookup table applies.
<i>eai:attributes</i>	Field control information.
<i>eai:data</i>	The source path for the lookup staging area. The lookup table file is moved from here into \$SPLUNK_HOME.
<i>eai:userName</i>	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:dict>
  </content>
</entry>
</s:messages>
```

```

        </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
<i>eai:data</i> 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
<i>eai:appName</i>	The app for which the lookup table applies.
<i>eai:data</i>	The source path for the lookup staging area. The lookup table file is moved from here into \$SPLUNK_HOME.
<i>eai:userName</i>	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
<i>attribute</i>	The name of the calculated field, which includes the "EVAL-" prefix.
<i>field.name</i>	The name of the field which is being calculated with an EVAL expression.
<i>stanza</i>	The name of the stanza in props.conf that defines the calculated field.
<i>type</i>	The type of the calculated field.

Name	Description
	This is always EVAL.
<i>value</i>	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>
</s:messages>
```

```

    </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
<i>name</i> 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.
<i>stanza</i> required	String		The name of the stanza in props.conf for the calculated field.  The name can be any of the following: <ul style="list-style-type: none"> <li>• Sourcetype of an event</li> <li>• host::&lt;host&gt;, where &lt;host&gt; is the host for an event</li> <li>• source::&lt;source&gt;, where &lt;source&gt; is the source for an event.</li> </ul> <b>Note:</b> Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.
<i>value</i> required	String		The eval statement, which can be evaluated to any value type, including multivalued, boolean, or null.  <b>Note:</b> Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.

### Returned values

Name	Description
<i>attribute</i>	The name of the calculated field, which includes the "EVAL-" prefix.
<i>field.name</i>	The name of the field which is being calculated with an EVAL expression.
<i>stanza</i>	The name of the stanza in props.conf that defines the calculated field.
<i>type</i>	The type of the calculated field.  This is always EVAL.
<i>value</i>	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
<i>attribute</i>	The name of the calculated field, which includes the "EVAL-" prefix.
<i>field.name</i>	The name of the field which is being calculated with an EVAL expression.
<i>stanza</i>	The name of the stanza in props.conf that defines the calculated field.
<i>type</i>	The type of the calculated field.  This is always EVAL.
<i>value</i>	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
<i>value</i>	String		<p>The eval statement, which can be evaluated to any value type, including multivals, boolean, or null.</p> <p><i>Note:</i> Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.</p> <p>See <a href="#">Create a calculated field by editing props.conf</a> in the <i>Knowledge Manager Manual</i> for details.</p>

## Returned values

Name	Description
<i>attribute</i>	The name of the calculated field, which includes the "EVAL-" prefix.
<i>field.name</i>	The name of the field which is being calculated with an EVAL expression.
<i>stanza</i>	The name of the stanza in props.conf that defines the calculated field.

Name	Description
<i>type</i>	The type of the calculated field.  This is always EVAL.
<i>value</i>	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
<i>attribute</i>	Specifies the field extraction configuration.  For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	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.
<i>type</i>	Specifies the field extraction type, which can be either <code>inline</code> or <code>uses transform</code> .
<i>value</i>	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
<i>name</i> required	String		The user-specified part of the field extraction name. The full name of the field extraction includes this identifier as a suffix.
<i>stanza</i> 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.
<i>type</i> required	Enum		Valid values: (REPORT   EXTRACT)  An EXTRACT-type field extraction is defined with an "inline" regular expression. A REPORT-type field extraction refers to a transforms.conf stanza.
<i>value</i> 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.

Name	Type	Default	Description

## Returned values

Name	Description
<i>attribute</i>	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	Specifies the name of the stanza for the field extraction.
<i>type</i>	Specifies the field extraction type, which can be either <code>inline</code> or <code>uses transform</code> .
<i>value</i>	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
<i>attribute</i>	Specifies the field extraction configuration. For example, REPORT- <code>&lt;name&gt;</code> or EXTRACT- <code>&lt;name&gt;</code> .
<i>stanza</i>	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.
<i>type</i>	Specifies the field extraction type, which can be either <code>inline</code> or <code>uses transform</code> .
<i>value</i>	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 ...
</feed>
```

```

<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
<i>value required</i>	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
<i>attribute</i>	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	Specifies the name of the stanza for the field extraction.
<i>type</i>	Specifies the field extraction type, which can be either <code>inline</code> or <code>uses transform</code> .
<i>value</i>	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
<i>alias.*</i>	The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
<i>attribute</i>	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	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.
<i>type</i>	Specifies the field extraction type, which can be either <code>inline</code> or <code>uses transform</code> .
<i>value</i>	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
<i>alias.*</i>	String		The alias for a given field. For example, supply a value of "bar" for an argument "alias.foo" to alias "foo" to "bar".
<i>name required</i>	String		The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
<i>stanza required</i>	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
<i>alias.*</i>	The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
<i>attribute</i>	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	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.
<i>type</i>	Specifies the field extraction type, which can be either inline or uses transform.
<i>value</i>	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
<i>alias.*</i>	The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.
<i>attribute</i>	Specifies the field extraction configuration.  For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	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.
<i>type</i>	Specifies the field extraction type, which can be either <code>inline</code> or <code>uses transform</code> .

Name	Description
<i>value</i>	<p>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields.</p> <p>If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</p>

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

```

... 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
<i>alias.*</i>	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
<i>alias.*</i>	The alias for a given field. For example, supply a value of "bar" for an argument "alias.foo" to alias "foo" to "bar".
<i>attribute</i>	Specifies the field extraction configuration. For example, REPORT-<name> or EXTRACT-<name>.
<i>stanza</i>	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.
<i>type</i>	Specifies the field extraction type, which can be either inline or uses transform.
<i>value</i>	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
<i>attribute</i>	Specifies the field extraction configuration.  For example, LOOKUP-my_lookup.
<i>overwrite</i>	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.
<i>stanza</i>	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.
<i>transform</i>	The transforms.conf stanza that defines the lookup to apply.
<i>type</i>	Specifies the field extraction type.  For this endpoint, this is always LOOKUP
<i>value</i>	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
<i>lookup.field.input.*</i>	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.
<i>lookup.field.output.*</i>	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
<i>name</i> required	String		The user-specified part of the automatic lookup name. The full name of the automatic lookup includes this identifier as a suffix.
<i>overwrite</i> 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.
<i>stanza</i> 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.
<i>transform</i> required	String		The transforms.conf stanza that defines the lookup to apply.

## Returned values

Name	Description
<i>attribute</i>	Specifies the field extraction configuration.  For example, LOOKUP-my_lookup.
<i>lookup.field.input.*</i>	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.
<i>lookup.field.output.*</i>	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.
<i>overwrite</i>	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.
<i>stanza</i>	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.
<i>transform</i>	The transforms.conf stanza that defines the lookup to apply.
<i>type</i>	Specifies the field extraction type.  For this endpoint, this is always LOOKUP.
<i>value</i>	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%203A%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
<i>attribute</i>	Specifies the field extraction configuration.  For example, LOOKUP-my_lookup.
<i>overwrite</i>	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.
<i>stanza</i>	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.
<i>transform</i>	The transforms.conf stanza that defines the lookup to apply.
<i>type</i>	Specifies the field extraction type.  For this endpoint, this is always LOOKUP.
<i>value</i>	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"/>
  </entry>
</feed>
```

```

    <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
<i>lookup.field.input.*</i>	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.
<i>lookup.field.output.*</i>	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.
<i>overwrite required</i>	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
<i>transform required</i>	String		The transforms.conf stanza that defines the lookup to apply.

## Returned values

Name	Description
<i>attribute</i>	Specifies the field extraction configuration. For example, LOOKUP-my_lookup.
<i>lookup.field.input.*</i>	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.
<i>lookup.field.output.*</i>	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.
<i>overwrite</i>	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.
<i>stanza</i>	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.
<i>transform</i>	The transforms.conf stanza that defines the lookup to apply.
<i>type</i>	Specifies the field extraction type. For this endpoint, this is always LOOKUP.
<i>value</i>	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
<i>attribute</i>	The configuration key.
<i>stanza</i>	The sourcetype to rename, which is the name of a stanza in props.conf.
<i>type</i>	The value of the configuration key.
<i>value</i>	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
<i>name</i> required	String		The original sourcetype name.
<i>value</i> required	String		The new sourcetype name.

### Returned values

Name	Description
<i>attribute</i>	The configuration key.
<i>stanza</i>	The sourcetype to rename, which is the name of a stanza in props.conf.
<i>type</i>	The value of the configuration key.
<i>value</i>	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
<i>attribute</i>	The configuration key.
<i>stanza</i>	The sourcetype to rename, which is the name of a stanza in props.conf.
<i>type</i>	The value of the configuration key.
<i>value</i>	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
<i>value</i> required	String		The new sourcetype name.

### Returned values

Name	Description
<i>attribute</i>	The configuration key.
<i>stanza</i>	The sourcetype to rename, which is the name of a stanza in props.conf.
<i>type</i>	The value of the configuration key.
<i>value</i>	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
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	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.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	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.
<i>KEEP_EMPTY_VALS</i>	If set to true, Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	Optional attribute for index-time field 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).
<i>MV_ADD</i>	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.
<i>REGEX</i>	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.
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	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.
<i>disabled</i>	Indicates if the field transformation is disabled.
<i>eai:appName</i>	The Splunk app for which the field extractions are defined. For example, the search app.
<i>eai:userName</i>	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 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
<i>CAN_OPTIMIZE</i>	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 <i>*always*</i> 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.
<i>CLEAN_KEYS</i>	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.
<i>disabled</i>	Boolean		Specifies whether the field transformation is disabled.
<i>FORMAT</i>	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
			<p>The special identifier \$0 represents what was in the DEST_KEY before the REGEX was performed.</p> <p>At index-time only, you can use FORMAT to create concatenated fields:  FORMAT = ipaddress::\$1.\$2.\$3.\$4</p> <p>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"</p> <p>At index-time, FORMAT defaults to &lt;stanza-name&gt;::\$1</p> <p>FORMAT for search-time extractions:</p> <p>The format of this field as used during search time extractions is as follows:  \tFORMAT = &lt;field-name&gt;::&lt;field-value&gt;( &lt;field-name&gt;::&lt;field-value&gt;)*  \tfield-name = [&lt;string&gt; \$&lt;extracting-group-number&gt;] \tfield-value = [&lt;string&gt; \$&lt;extracting-group-number&gt;]</p> <p>Search-time extraction examples: \tFORMAT = first::\$1 second::\$2 third::other-value \tFORMAT = \$1::\$2</p> <p>You cannot create concatenated fields with FORMAT at search time. That functionality is only available at index time.</p> <p>At search-time, FORMAT defaults to an empty string.</p>
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		<p>Specify a regular expression to operate on your data.</p> <p>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.</p> <p>REGEX and the FORMAT attribute:</p> <p>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.</p>



Name	Description
	For details, see the documentation for this parameter in the POST operation.
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	<p>Indicates whether to automatically write REGEX to metadata.</p> <p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>disabled</i>	Indicates if the field transformation is disabled.
<i>eai:appName</i>	The Splunk app for which the field extractions are defined. For example, the search app.
<i>eai:userName</i>	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"/>
  </entry>
</feed>
```

```

<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
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	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.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	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.
<i>KEEP_EMPTY_VALS</i>	If set to true, Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	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).
<i>MV_ADD</i>	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.
<i>REGEX</i>	<p>The regular expression to operate on your data.</p> <p>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.</p> <p>For details, see the documentation for this parameter in the POST operation.</p>
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	<p>Indicates whether to automatically write REGEX to metadata.</p> <p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>disabled</i>	Indicates if the field transformation is disabled.
<i>eai:appName</i>	The Splunk app for which the field extractions are defined. For example, the search app.
<i>eai:attributes</i>	Field control information.
<i>eai:userName</i>	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 ...
</feed>
```

```

<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
<i>REGEX</i>	String		<p>Specify a regular expression to operate on your data.</p> <p>This attribute is valid for both index-time and search-time field extractions: <code>\tREGEX</code> is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use <code>DELIMS</code> (see the <code>DELIMS</code> attribute description, below). <code>\tREGEX</code> is required for all index-time transforms.</p> <p>REGEX and the <code>FORMAT</code> attribute:</p> <p>Name-capturing groups in the REGEX are extracted directly to fields. This means that you do not need to specify the <code>FORMAT</code> attribute for simple field extraction cases.</p> <p>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 <code>FORMAT</code>: <code>_KEY_&lt;string&gt;</code>, <code>_VAL_&lt;string&gt;</code>.</p> <p>For example, the following are equivalent: <code>\tUsing FORMAT: \t\tREGEX = ([a-z]+)=([a-z]+) \t\tFORMAT = \$1::\$2 \tWithout using FORMAT \t\tREGEX = (?&lt;_KEY_1&gt;[a-z]+)=(?&lt;_VAL_1&gt;[a-z]+)</code></p> <p>REGEX defaults to an empty string.</p>
<i>SOURCE_KEY</i>	String	<code>_raw</code>	Specify the KEY to which Splunk software applies REGEX.
<i>CAN_OPTIMIZE</i>	Bool	True	<p>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.</p> <p>NOTE: This option should rarely be set to false.</p>
<i>CLEAN_KEYS</i>	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.
<i>FORMAT</i>	String		This option is valid for both index-time and search-time field extractions. However, <code>FORMAT</code> behaves differently depending on whether the extraction is performed at index time or search time.

Name	Type	Default	Description
			<p>This attribute specifies the format of the event, including any field names or values you want to add.</p> <p>FORMAT for index-time extractions:</p> <p>Use \$n (for example \$1, \$2, etc) to specify the output of each REGEX match.</p> <p>If REGEX does not have n groups, the matching fails.</p> <p>The special identifier \$0 represents what was in the DEST_KEY before the REGEX was performed.</p> <p>At index-time only, you can use FORMAT to create concatenated fields: FORMAT = ipaddress::\$1.\$2.\$3.\$4</p> <p>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"</p> <p>At index-time, FORMAT defaults to &lt;stanza-name&gt;::\$1</p> <p>FORMAT for search-time extractions:</p> <p>The format of this field as used during search time extractions is as follows: \tFORMAT = &lt;field-name&gt;::&lt;field-value&gt;( &lt;field-name&gt;::&lt;field-value&gt;)*  \tfield-name = [&lt;string&gt; \$&lt;extracting-group-number&gt;]  \tfield-value = [&lt;string&gt; \$&lt;extracting-group-number&gt;]</p> <p>Search-time extraction examples: \tFORMAT = first::\$1 second::\$2 third::other-value \tFORMAT = \$1::\$2</p> <p>You cannot create concatenated fields with FORMAT at search time. That functionality is only available at index time.</p> <p>At search-time, FORMAT defaults to an empty string.</p>
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
<i>disabled</i>	Boolean		Specifies whether the field transformation is disabled.

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.

## Returned values

Name	Description
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	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.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	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.
<i>KEEP_EMPTY_VALS</i>	If set to true, Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	Optional attribute for index-time field 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).
<i>MV_ADD</i>	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.
<i>REGEX</i>	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
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	<p>Indicates whether to automatically write REGEX to metadata.</p> <p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>disabled</i>	Indicates if the field transformation is disabled.
<i>eai:appName</i>	The Splunk app for which the field extractions are defined. For example, the search app.
<i>eai:userName</i>	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
<i>getsize</i>	Boolean	false	Enable to return the file size.
<i>replicate_delta</i>	Boolean	false	Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.

### Returned values

Name	Description
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	

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.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	<p>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.</p> <p>This attribute specifies the format of the event, including any field names or values you want to add.</p> <p>For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.</p>
<i>GETSIZE</i>	If enabled, returns the file size.
<i>KEEP_EMPTY_VALS</i>	If set to true, Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	<p>Optional attribute for index-time field extractions. specifies how many characters to search into an event.</p> <p>Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</p>
<i>MV_ADD</i>	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.
<i>REGEX</i>	<p>The regular expression to operate on your data.</p> <p>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.</p> <p>For details, see the documentation for this parameter in the POST operation.</p>
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	<p>Indicates whether to automatically write REGEX to metadata.</p> <p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>disabled</i>	Indicates if this lookup is disabled.
<i>eai:appName</i>	The Splunk app for which the lookups are defined. For example, the search app.
<i>eai:userName</i>	The Splunk user for which the lookups are defined.
<i>external_cmd</i>	<p>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.</p> <p>This string is parsed like a shell command. The first argument is expected to be a python script located in:</p>



Name	Description
	\$SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.
<i>fields_list</i>	List of all fields that are supported by the external command.
<i>replicate_delta</i>	Indicates that only the changes to a CSV lookup table are replicated, rather than the entire lookup table.
<i>type</i>	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:dict>
    </content>
  </entry>
</feed>
```

```

<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
<i>collection</i>	String	<empty>	Name of the collection to use for this lookup. The collection should be defined in <code>\$SPLUNK_HOME/etc/&lt;app_name&gt;/collections.conf</code> for the current app.  To create a KV Store lookup, use <code>collection</code> to pass in the KV Store collection name and include the <code>external_type</code> parameter with a value of <code>kvstore</code> in your POST request.
<i>name</i>	String		The name of the lookup definition.
<i>default_match</i>	String		If <code>min_matches</code> is greater than zero and Splunk software has less than <code>min_matches</code> for any given input, it provides this <code>default_match</code> value one or more times until the <code>min_matches</code> threshold is reached.
<i>disabled</i>	Boolean		Specifies whether the lookup definition is disabled.
<i>external_cmd</i>	String		Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface 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:  <code>\$SPLUNK_HOME/etc/&lt;app_name&gt;/bin</code> (or <code>../etc/searchscripts</code> )  Presence of this field indicates that the lookup is external and command based.
<i>external_type</i>	One of the following values: <ul style="list-style-type: none"><li>python</li><li>executable</li><li>geo</li><li>kvstore</li></ul>	python	Type of external command for performing a lookup.  To define a KV Store lookup, use <code>external_type = kvstore</code> . Include the KV Store <code>collection</code> name in your POST request.
<i>fields_list</i>	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
<i>filename</i>	String		The name of the static lookup table file.
<i>max_matches</i>	Number		The maximum number of possible matches for each input lookup value.
<i>max_offset_secs</i>	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.
<i>min_matches</i>	Number		The minimum number of possible matches for each input lookup value.
<i>min_offset_secs</i>	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.
<i>replicate_delta</i>	Boolean	false	Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.
<i>time_field</i>	String		For temporal lookups, this is the field in the lookup table that represents the timestamp.
<i>time_format</i>	String		For temporal lookups, this specifies the "strptime" format of the timestamp field.

## Returned values

Name	Description
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	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.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	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.
<i>KEEP_EMPTY_VALS</i>	If set to true, Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	Optional attribute for index-time field 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).
<i>MV_ADD</i>	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.
<i>REGEX</i>	The regular expression to operate on your data.

Name	Description
	<p>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.</p> <p>For details, see the documentation for this parameter in the POST operation.</p>
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	<p>Indicates whether to automatically write REGEX to metadata.</p> <p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>default_match</i>	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.
<i>disabled</i>	Specifies whether the lookup definition is disabled.
<i>eai:appName</i>	The Splunk app for which the lookups are defined. For example, the search app.
<i>eai:userName</i>	The Splunk user for which the lookups are defined.
<i>external_cmd</i>	<p>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.</p> <p>This string is parsed like a shell command. The first argument is expected to be a python script located in:</p> <p><code>\$SPLUNK_HOME/etc/&lt;app_name&gt;/bin (or ../etc/searchscripts)</code></p> <p>Presence of this field indicates that the lookup is external and command based.</p>
<i>fields_list</i>	List of all fields that are supported by the external command. Use this for external (or "scripted") lookups.
<i>filename</i>	The name of the static lookup table file.
<i>max_matches</i>	<p>The maximum number of possible matches for each input lookup value.</p> <p>If the lookup is non-temporal (not time-bounded, meaning the time_field attribute is not specified), Splunk software uses the first &lt;integer&gt; entries, in file order.</p> <p>If the lookup is temporal, Splunk software uses the first &lt;integer&gt; entries in descending time order.</p> <p>Default = 100 if the lookup is not temporal, default = 1 if it is temporal.</p>
<i>max_offset_secs</i>	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.
<i>min_matches</i>	The minimum number of possible matches for each input lookup value.
<i>min_offset_secs</i>	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.
<i>time_field</i>	For temporal lookups, this is the field in the lookup table that represents the timestamp.

Name	Description
<i>time_format</i>	For temporal lookups, this specifies the "\\strptime\\" format of the timestamp field.
<i>type</i>	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:dict>
    </content>
  </entry>
</feed>
```

```

    <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
<i>replicate_delta</i>	Boolean	false	Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.

### Returned values

Name	Description
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	Indicates whether Splunk software "cleans" the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	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.
<i>KEEP_EMPTY_VALS</i>	Indicates whether Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	For index-time field 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).
<i>MV_ADD</i>	"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.
<i>REGEX</i>	The regular expression to operate on your data.

Name	Description
	<p>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.</p> <p>For details, see the documentation for this parameter in the POST operation.</p>
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	<p>Indicates whether to automatically write REGEX to metadata.</p> <p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>disabled</i>	Indicates if this lookup is disabled.
<i>eai:appName</i>	The Splunk software app for which the lookups are defined. For example, the search app.
<i>eai:attributes</i>	Field control information.
<i>eai:userName</i>	The Splunk user for which the lookups are defined.
<i>filename</i>	The name of the static lookup table file.
<i>replicate_delta</i>	Indicates that only the changes to a CSV lookup table are replicated, rather than the entire lookup table.
<i>type</i>	<p>Specifies the field extraction type.</p> <p>Can be either external or file.</p>

## 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
<i>collection</i>	String	<empty>	Name of the collection to use for this lookup. The collection should be defined in <code>\$\$SPLUNK_HOME/etc/&lt;app_name&gt;/collections.conf</code> for the current app.  To create a KV Store lookup, use <code>collection</code> to pass in the KV Store collection name and include the <code>external_type</code> parameter with a value of <code>kvstore</code> in your POST request.
<i>default_match</i>	String		If <code>min_matches</code> is greater than zero and Splunk software has less than <code>min_matches</code> for any given input, it provides this <code>default_match</code> value one or more times until the <code>min_matches</code> threshold is reached.
<i>disabled</i>	Boolean		Specifies whether the lookup definition is disabled.
<i>external_cmd</i>	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:  <code>\$\$SPLUNK_HOME/etc/&lt;app_name&gt;/bin</code> (or <code>../etc/searchscripts</code> )  Presence of this field indicates that the lookup is external and command based.
<i>external_type</i>	One of the following values: <ul style="list-style-type: none"><li>• <code>python</code></li><li>• <code>executable</code></li><li>• <code>geo</code></li><li>• <code>kvstore</code></li></ul>	<code>python</code>	Type of external command for performing a lookup.  To define a KV Store lookup, use  <code>external_type = kvstore</code> . Include the KV Store <code>collection</code> name in your POST request.
<i>fields_list</i>	String		A comma- and space-delimited list of all fields that are supported by the external command. Use this for external (or "scripted") lookups.
<i>filename</i>	String		The name of the static lookup table file.
<i>max_matches</i>	Number		The maximum number of possible matches for each input lookup value.
<i>max_offset_secs</i>	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.
<i>min_matches</i>	Number		The minimum number of possible matches for each input lookup value.
<i>min_offset_secs</i>	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.
<i>replicate_delta</i>	Boolean	<code>false</code>	

Name	Type	Default	Description
			Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.
<i>time_field</i>	String		For temporal lookups, this is the field in the lookup table that represents the timestamp.
<i>time_format</i>	String		For temporal lookups, this specifies the "strptime" format of the timestamp field.

## Returned values

Name	Description
<i>CAN_OPTIMIZE</i>	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 <i>always</i> 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.
<i>CLEAN_KEYS</i>	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.
<i>DEFAULT_VALUE</i>	Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.
<i>DEST_KEY</i>	Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.
<i>FORMAT</i>	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.
<i>KEEP_EMPTY_VALS</i>	If set to true, Splunk software preserves extracted fields with empty values.
<i>LOOKAHEAD</i>	Optional attribute for index-time field 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).
<i>MV_ADD</i>	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.
<i>REGEX</i>	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.
<i>SOURCE_KEY</i>	The KEY to which Splunk software applies REGEX.
<i>WRITE_META</i>	Indicates whether to automatically write REGEX to metadata.

Name	Description
	<p>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).</p> <p>Use instead of DEST_KEY = meta.</p>
<i>default_match</i>	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.
<i>disabled</i>	Specifies whether the lookup definition is disabled.
<i>eai:appName</i>	The Splunk app for which the lookups are defined. For example, the search app.
<i>eai:userName</i>	The Splunk user for which the lookups are defined.
<i>external_cmd</i>	<p>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.</p> <p>This string is parsed like a shell command. The first argument is expected to be a python script located in:</p> <p>\$SPLUNK_HOME/etc/&lt;app_name&gt;/bin (or ../etc/searchscripts)</p> <p>Presence of this field indicates that the lookup is external and command based.</p>
<i>fields_list</i>	List of all fields that are supported by the external command. Use this for external (or "scripted") lookups.
<i>filename</i>	The name of the static lookup table file.
<i>max_matches</i>	The maximum number of possible matches for each input lookup value.
<i>max_offset_secs</i>	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.
<i>min_matches</i>	The minimum number of possible matches for each input lookup value.
<i>min_offset_secs</i>	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.
<i>time_field</i>	For temporal lookups, this is the field in the lookup table that represents the timestamp.
<i>time_format</i>	For temporal lookups, this specifies the "strftime" format of the timestamp field.
<i>type</i>	<p>Specifies the field extraction type.</p> <p>Can be either external or file.</p>

## 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>2011-07-21T20:00:07:00</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>2011-07-21T20:00:07:00</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
<i>name</i> required	String	Required. Name of the <code>metric-schema</code> stanza in <code>transforms.conf</code> .
<i>field_name</i> required	String	Comma-separated list of measure fields to be extracted from a log line.
<i>blacklist_dimension</i> optional	String	Comma-separated list of dimension fields to be omitted when log events are converted to metric data points.
<i>metric_name_prefix</i> 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
<i>METRIC-SCHEMA-MEASURES-&lt;metric_name_prefix&gt;</i>	String	Comma-separated list of measure fields to be extracted from a log line.
<i>METRIC-SCHEMA-BLACKLIST-DIMS-&lt;metric_name_prefix&gt;</i>	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
<i>unique_transforms_stanza_name</i>	String	A unique name for this stanza.
<i>REGEX</i> = <i>&lt;regular expression&gt;</i>	String	A regular expression that defines how to match and extract dimensions from StatsD metrics data. Splunk supports a named capturing-group extraction format ( <i>?&lt;dim1&gt;group</i> ) ( <i>?dim2&gt;group</i> ) ... to provide dimension names for the corresponding values that are extracted.
<i>REMOVE_DIMS_FROM_METRIC_NAME</i> = <i>&lt;Boolean&gt;</i>	Boolean	<p>Specifies whether unmatched segments of the StatsD dotted name segment are used as the <i>metric_name</i>.</p> <p>When <i>true</i>, dimension values are be removed from the measurement and the unmatched portion becomes the <i>metric_name</i>. The default value is <i>true</i>.</p> <p>When <i>false</i>, extracted dimension values are included in the <i>metric_name</i>.</p> <p>For example, a metric measurement name is "x.y.z". The regular expression matches "y" and "z". When <i>REMOVE_DIMS_FROM_METRIC_NAME</i> is <i>true</i>, <i>metric_name</i> is "x". When <i>false</i>, <i>metric_name</i> is "x.y.z".</p>

## 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
<i>background_color</i>	Indicates the color of the banner.
<i>hyperlink</i>	The link included in the banner.
<i>hyperlink_text</i>	Display text for the link in the banner.
<i>message</i>	Banner notification text.
<i>visible</i>	Boolean value indicating whether the banner is visible.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

```

    <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
<i>background_color</i> required	String	blue	Indicates the color of the banner. The color can be any of the following: <ul style="list-style-type: none"> <li>• green</li> <li>• blue</li> <li>• yellow</li> <li>• orange</li> <li>• red</li> </ul>
<i>hyperlink</i> optional	String		The link included in the banner. The link must begin with <code>http://</code> or <code>https://</code> .
<i>hyperlink_text</i> optional	String		Display text for the link in the banner.
<i>message</i> required	String	<i>sample text</i>	Banner notification text.
<i>visible</i> required	Boolean	false	Indicates whether the banner is visible.

## Returned values

Name	Description
<i>background_color</i>	Indicates the color of the banner.
<i>hyperlink</i>	The link included in the banner.
<i>hyperlink_text</i>	Display text for the link in the banner.
<i>message</i>	Banner notification text.
<i>visible</i>	Boolean value indicating whether the banner is visible.

## Example request and response

### XML Request

```
curl -X POST -k -u admin:pass https://localhost:8089/services/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>:<port>/servicesNS/{user}/{app\\_name}/data/ui/panels](https://<host>:<port>/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
<i>eai:appName</i>	App context for the panel.
<i>eai:data</i>	XML definition for the panel.
<i>eai:userName</i>	User who created the panel.
<i>label</i>	Panel label.



Name	Description
<i>panel.title</i>	Panel title.
<i>rootNode</i>	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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</panels>
```

```

        <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">1c70628bb4aee0470707e59e1b2d321</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
<i>name</i>	String		Panel name.
<i>eai:data</i>	XML document		Panel XML definition.

### Returned values

Name	Description
<i>eai:appName</i>	App context for the panel.
<i>eai:data</i>	XML definition for the panel.
<i>eai:userName</i>	User who created the panel.
<i>label</i>	Panel label.
<i>panel.title</i>	Panel title.
<i>rootNode</i>	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">1c70628bb4aee0470707e59e1b2d321</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
<i>eai:appName</i>	App context for the dashboard.
<i>eai:data</i>	XML definition for the dashboard.
<i>eai:type</i>	User interface type. For dashboards, this type is <code>view</code> .
<i>eai:userName</i>	User who created the dashboard.
<i>isDashboard</i>	Boolean value indicating whether the knowledge object is a dashboard.
<i>isVisible</i>	Boolean value indicating whether the dashboard is visible.
<i>label</i>	Dashboard label.
<i>rootNode</i>	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="a1c9b18fdcf" 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
<i>name</i>	String		Dashboard name.
<i>eai:data</i>	XML document		Dashboard XML definition.

### Returned values

Name	Description
<i>eai:appName</i>	App context for the dashboard.
<i>eai:data</i>	XML definition for the dashboard.
<i>eai:type</i>	User interface type. For dashboards, this type is <code>view</code> .
<i>eai:userName</i>	User who created the dashboard.
<i>isDashboard</i>	Boolean value indicating whether the knowledge object is a dashboard.
<i>isVisible</i>	Boolean value indicating whether the dashboard is visible.
<i>label</i>	Dashboard label.
<i>rootNode</i>	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="a1c9b18fdcf" 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}](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
<i>eai:appName</i>	App context for the dashboard.
<i>eai:data</i>	XML definition for the dashboard.
<i>eai:type</i>	User interface type. For dashboards, this type is <code>view</code> .
<i>eai:userName</i>	User who created the dashboard.
<i>isDashboard</i>	Boolean value indicating whether the knowledge object is a dashboard.
<i>isVisible</i>	Boolean value indicating whether the dashboard is visible.
<i>label</i>	Dashboard label.
<i>rootNode</i>	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="a1c9b18fdcf" 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
<i>eai:data</i>	XML document		Dashboard XML definition.

### Returned values

Name	Description
<i>eai:appName</i>	App context for the dashboard.
<i>eai:data</i>	XML definition for the dashboard.
<i>eai:type</i>	User interface type. For dashboards, this type is <code>view</code> .
<i>eai:userName</i>	User who created the dashboard.
<i>isDashboard</i>	Boolean value indicating whether the knowledge object is a dashboard.
<i>isVisible</i>	Boolean value indicating whether the dashboard is visible.
<i>label</i>	Dashboard label.
<i>rootNode</i>	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 -d "eai:data=<dashboard><label>new_label</label></dashboard>"
```

#### XML Response

```
<title>views</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
<updated>2015-10-08T16:38:23-07:00</updated>
<generator build="a1c9b18fdcf" version="6.4.0"/>
<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>2015-10-08T16:38:23-07:00</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:data"><![CDATA[<dashboard><label>new_label</label></dashboard>]]></s:key>
    <s:key name="eai:digest">31513ad6cce14b5c792f175cc1691e5e</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">new_label</s:key>
    <s:key name="rootNode">dashboard</s:key>
  </s:dict>
</content>

```

## DELETE

Delete a specific dashboard XML definition.

## Request parameters

None.

## Returned values

None.

## Example request and response

## XML Request

```
curl -k -u username:password --request DELETE
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>2015-10-08T17:07:12-07:00</updated>
<generator build="alc9b18fdcf" 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>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s: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
<i>acceleration</i>	Indicates if acceleration is enabled for this data model.
<i>acceleration.earliest_time</i>	The earliest time to dispatch the search.
<i>search</i>	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:dict>
    </s:key>
  </entry>
</feed>
```

```

<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
<i>concise</i>	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
<i>acceleration</i>	Indicates whether acceleration is enabled for the data model.
<i>concise</i>	Indicates whether to list a concise JSON description of the data model.
<i>description</i>	The JSON describing the data model.
<i>displayName</i>	The name displayed for the data model in Splunk Web.
<i>eai:appName</i>	The Splunk app in which the data model was created.
<i>eai:userName</i>	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:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

        <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
<i>description</i>	String		JSON description of the data model.
<i>name</i>	String		Name of the data model.
<i>acceleration</i>	String		<p>Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.</p> <ul style="list-style-type: none"> <li>• <i>enabled</i> (true or false)</li> <li>• <i>earliest_time</i> (time modifier)</li> <li>• <i>cron_schedule</i> (cron string)</li> </ul> <p><b>Example</b></p> <pre>acceleration= ' {   "enabled": true,   "earliest_time": -1mon,   "cron_schedule": 0 */12 * * * } '</pre>
Hunk data model acceleration settings	See description		<p>Use these settings to configure acceleration for Hunk data models.</p> <ul style="list-style-type: none"> <li>• <i>hunk.compression_codec</i></li> </ul> <p>String, case-sensitive.</p>



Name	Type	Default	Description
			<p>Specifies the compression codec to be used for the accelerated orc or parquet format files. For <code>parquet</code> file format, use <code>snappy</code> or <code>gzip</code>. For <code>orc</code> file format, use <code>snappy</code> or <code>zlib</code>.</p> <ul style="list-style-type: none"> <li>• <code>hunk.dfs_block_size</code></li> </ul> <p>Unsigned integer Specifies the block size in bytes for the compression files.</p> <ul style="list-style-type: none"> <li>• <code>hunk.file_format</code></li> </ul> <p>String, case sensitive. Valid options are <code>orc</code> and <code>parquet</code></p> <p><b>Example</b></p> <pre>acceleration= ' {   "hunk.file_format": "orc",   "hunk.compression_codec": "snappy" } '</pre>

## 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">05calal93365a3b613b919c6401591e3</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
<i>concise</i>	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
<i>acceleration</i>	Indicates whether acceleration is enabled for the data model.
<i>concise</i>	Indicates whether to list a concise JSON description of the data model.
<i>description</i>	The JSON describing the data model.
<i>displayName</i>	The name displayed for the data model in Splunk Web.

Name	Description
<i>eai:appName</i>	The Splunk app in which the data model was created.
<i>eai:attributes</i>	Field control information.
<i>eai:userName</i>	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
<i>acceleration</i>	String		<p>Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.</p> <ul style="list-style-type: none"> <li>• <i>enabled</i> (true or false)</li> <li>• <i>earliest_time</i> (time modifier)</li> <li>• <i>cron_schedule</i> (cron string)</li> </ul> <p><b>Example</b></p> <pre>acceleration= ' {   "enabled": true,   "earliest_time": -1mon,   "cron_schedule": 0 */12 * * * } '</pre>
Hunk data model acceleration settings	See description		<p>Use these settings to configure acceleration for Hunk data models.</p> <ul style="list-style-type: none"> <li>• <i>hunk.compression_codec</i></li> </ul> <p>String, case-sensitive.</p>

Name	Type	Default	Description
			<p>Specifies the compression codec to be used for the accelerated orc or parquet format files. For <code>parquet</code> file format, use <code>snappy</code> or <code>gzip</code>. For <code>orc</code> file format, use <code>snappy</code> or <code>zlib</code>.</p> <ul style="list-style-type: none"> <li>• <code>hunk.dfs_block_size</code></li> </ul> <p>Unsigned integer Specifies the block size in bytes for the compression files.</p> <ul style="list-style-type: none"> <li>• <code>hunk.file_format</code></li> </ul> <p>String, case sensitive. Valid options are <code>orc</code> and <code>parquet</code></p> <p><b>Example</b></p> <pre>acceleration= ' {   "hunk.file_format": "orc",   "hunk.compression_codec": "snappy" } '</pre>
<i>description</i>	String		JSON description of the data model.
<i>provisional</i>	Boolean		<p>Indicates whether the data model is provisional. Provisional data models are not saved.</p> <p>Specify true to validate a data model before saving it.</p> <p>If the endpoint returns with no errors, then specify this endpoint again, with <code>provisional</code> set to false, to save the data model.</p>

## Returned values

Name	Description
<i>acceleration</i>	Indicates whether acceleration is enabled for the data model.
<i>concise</i>	Indicates whether to list a concise JSON description of the data model.
<i>description</i>	The JSON describing the data model.
<i>displayName</i>	The name displayed for the data model in Splunk Web.
<i>eai:appName</i>	The Splunk app in which the data model was created.
<i>eai:attributes</i>	Field control information.
<i>eai:userName</i>	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
<i><code>pivot_json</code></i>	String		JSON specifying a pivot based on the named data model.  Typically, you URL encode this parameter.  This endpoint requires either this <code>pivot_json</code> parameter or a <code>pivot_search</code> parameter.
<i><code>pivot_search</code></i>	String		A pivot search command based on the named data model.  Typically, you URL encode this parameter.  This endpoint requires either a <code>pivot_json</code> or this <code>pivot_search</code> parameter.

### Returned values

Name	Description
<i><code>drilldown_search</code></i>	The search for running this pivot report using drilldown
<i><code>open_in_search</code></i>	Equivalent to search parameter, but listed more simply.
<i><code>pivot_json</code></i>	JSON specifying a pivot based on the named data model.
<i><code>pivot_search</code></i>	A pivot search command based on the named data model.
<i><code>search</code></i>	The search string for running the pivot report
<i><code>tstats_search</code></i>	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>
```

```
</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
<i>eai:type</i>	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

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
<i>description</i>	Description of this event type.

Name	Description
<i>disabled</i>	Indicates if the event type is disabled.
<i>eai:appName</i>	The Splunk app for which this event type applies. For example, the Splunk search app.
<i>eai:userName</i>	Splunk user name of the creator of this event type. For example, the Splunk admin user.
<i>priority</i>	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
<i>search</i>	Search terms for this event type.
<i>tags</i>	[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:dict>
    </content>
  </entry>
</feed>
```

```

    <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
<i>name</i>	String		The name for the event type.
<i>search</i>	String		Search terms for this event type.
<i>description</i>	String		Human-readable description of this event type.
<i>disabled</i>	Boolean	0	If True, disables the event type.
<i>priority</i>	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.
<i>tags</i>	String		[Deprecated] Use <code>tags.conf.spec</code> file to assign tags to groups of events with related field values.

Returned values

Name	Description
<i>description</i>	Description of this event type.
<i>disabled</i>	Indicates if this event type is disabled.
<i>eai:appName</i>	The Splunk app for which this event type applies. For example, the Splunk search app.
<i>eai:userName</i>	Splunk user name of the creator of this event type. For example, the Splunk admin user.
<i>priority</i>	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
<i>search</i>	Search terms for this event type.
<i>tags</i>	[Deprecated] Tags associated with this event type.  Use <code>tags.conf.spec</code> 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

`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
<i>description</i>	Description of this event type.
<i>disabled</i>	Indicates if the event type is disabled.
<i>eai:appName</i>	The Splunk app for which this event type applies. For example, the Splunk search app.
<i>eai:userName</i>	Splunk user name of the creator of this event type. For example, the Splunk admin user.
<i>priority</i>	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
<i>search</i>	Search terms for this event type.
<i>tags</i>	[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:dict>
  </content>
</entry>
</feed>

```

## POST

Create an event type.

## Request parameters

Name	Type	Default	Description
<i>name</i>	String		The name for the event type.
<i>search</i>	String		Search terms for this event type.
<i>description</i>	String		Human-readable description of this event type.
<i>disabled</i>	Boolean	0	If True, disables the event type.
<i>priority</i>	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.

Name	Type	Default	Description
<i>tags</i>	String		[Deprecated] Use <code>tags.conf.spec</code> file to assign tags to groups of events with related field values.

## Returned values

Name	Description
<i>description</i>	Description of this event type.
<i>disabled</i>	Indicates if this event type is disabled.
<i>eai:appName</i>	The Splunk app for which this event type applies. For example, the Splunk search app.
<i>eai:userName</i>	Splunk user name of the creator of this event type. For example, the Splunk admin user.
<i>priority</i>	The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.
<i>search</i>	Search terms for this event type.
<i>tags</i>	[Deprecated] Tags associated with this event type. Use <code>tags.conf.spec</code> 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"/>
  </entry>
</feed>
```

```

<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>

```

```
</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 <code>tags.conf.spec</code> 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 <code>tags.conf.spec</code> 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 `$SPLUNK_HOME/etc/system/default/fields.conf`, with overridden values in `$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>
</feed>
```

```

<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_VALUE      Attr:INDEXED      True
    Attr:TOKENIZER          False
  </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
<i>value</i>	String		The specific field value on which to bind the tags.
<i>add</i>	String		The tag to attach to this <code>field_name:value</code> combination.
<i>delete</i>	String		The tag to remove to this <code>field_name::value</code> 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
<i>add</i>	String		A field:value pair to tag with {tag_name}.
<i>delete</i>	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 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.

---

## 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 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

`https://<host>:<mPort>/services/kvstore/backup/create`

### POST

Create a KV Store backup archive file.

### Usage details

#### Request parameters

Name	Type	Description
<i>archive_name</i>	String	Specify a file name for the backup.
<i>appname_name</i>	String	Specify a target collection for backup, rather than all of the KV Store. Only available if <i>pointInTime</i> is not set to true.
<i>collection_name</i>	String	Specify a target app for backup, rather than all of the KV Store. Only available if <i>pointInTime</i> is not set to true.
<i>pointInTime</i>	Boolean	Defaults to false. To take a consistent backup, set it to true. Only available for single-instance deployments.
<i>cancel</i>	Boolean	Defaults to false. Set it to true to cancel an in-progress backup. Only available if <i>pointInTime</i> is set to true.
<i>parallelCollections</i>	Number	Defaults to 1. Raise the number to increase the number of collections to back up in parallel. Only available if <i>pointInTime</i> is set to true.

#### Returned values

Name	Description
<i>status</i>	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="dbd2996dbabd8f6751329c845684e0ffc9dlcca3" 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

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
<i>archive_name</i>	String	<b>Required.</b> Specifies the name of the backup file.
<i>appname_name</i>	String	Specify a target collection to restore, rather than the entire contents of the archive file. Only available if <i>pointInTime</i> not set to true.
<i>collection_name</i>	String	Specify a target app to restore, rather than the entire contents of the archive file. Only available if <i>pointInTime</i> not set to true.
<i>pointInTime</i>	Boolean	Defaults to false. To restore from a backup taken with consistency, set it to true.
<i>cancel</i>	Boolean	Defaults to false. Set it to true to cancel an in-progress restore. Only available if <i>pointInTime</i> set to true.
<i>parallelCollections</i>	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 <i>pointInTime</i> set to true.
<i>insertionsWorkersPerCollection</i>	Number	Defaults to 1. Raise to increase the number of insertion workers per collection, which speeds up the restore. Only available if <i>pointInTime</i> set to true.

#### Returned values

Name	Description
<i>status</i>	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="dbd2996dbabd8f6751329c845684e0ffc9dlcca3" 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

`https://<host>:<mPort>/services/kvstore/control/maintenance`

Access KV store maintenance mode for standalone deployments. This endpoint is not available for clustered deployments.

### POST

Toggle maintenance mode.

### Request parameters

Name	Type	Description
<i>mode</i>	Boolean	<b>Required.</b> Type <i>true</i> to enter maintenance mode. To exit, type <i>false</i> .

### 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
<i>current</i>	<p>Includes the following indicators for the machine making the GET request.</p> <ul style="list-style-type: none"> <li>• <code>backupRestoreStatus</code>: Status for a KV Store backup in progress. One of the following values:               <ul style="list-style-type: none"> <li>◆ <code>Busy</code>: Backup or restore in progress.</li> <li>◆ <code>Failed</code>: Restore failed to extract an archive file.</li> <li>◆ <code>Ready</code>: Ready to run a backup or restore.</li> <li>◆ <code>Shutdown</code>: KV Store is in the process of shutting down.</li> </ul> </li> <li>• <code>backupRestoreProgress</code>: Counter that increments each time a collection finishes being backed up or restored.</li> <li>• <code>date</code>: <code>DateTime</code> when this status was retrieved.</li> <li>• <code>datesec</code>: Unix timestamp, equivalent to <code>date</code></li> </ul>



Name	Description
	<ul style="list-style-type: none"> <li>• <b>disabled</b>: If KV Store is disabled on the current member. 0 means enabled, 1 means disabled.</li> <li>• <b>guid</b>: Instance ID of the current member.</li> <li>• <b>oplogEndTimestamp</b>: 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.</li> <li>• <b>oplogEndTimestampSec</b>: Unix timestamp equivalent to <code>oplogEndTimestamp</code></li> <li>• <b>oplogStartTimestamp</b>: First recorded timestamp in the operations log.</li> <li>• <b>oplogStartTimestampSec</b>: Unix timestamp equivalent to <code>oplogStartTimestamp</code></li> <li>• <b>port</b>: KV Store port</li> <li>• <b>replicaSet</b>: Replica set name. Instance ID by default for standalone mode. Configured in <code>server.conf</code> for SHC.</li> <li>• <b>replicationStatus</b>: In standalone mode, this is KV Store captain. Otherwise, one of the following values. <ul style="list-style-type: none"> <li>◆ Startup</li> <li>◆ KV Store captain</li> <li>◆ Non-captain KV Store member</li> <li>◆ Recovering</li> <li>◆ Initial Sync</li> <li>◆ Unknown status</li> <li>◆ Down</li> <li>◆ Rollback</li> <li>◆ Removed</li> </ul> </li> <li>• <b>standalone</b>: Indicates whether the machine making the request is a standalone member or SHC member. 1 indicates a standalone member.</li> <li>• <b>status</b>: KV Store status. One of the following values. <ul style="list-style-type: none"> <li>◆ unknown</li> <li>◆ disabled</li> <li>◆ starting</li> <li>◆ ready</li> <li>◆ failed</li> <li>◆ shuttingdown</li> </ul> </li> </ul>
<i>Enabled KV Store members</i>	<p>Returned for SHC deployments. Lists the following values for SHC members where KV Store is enabled and used for replication.</p> <ul style="list-style-type: none"> <li>• <b>guid</b>: Instance ID of the current member.</li> <li>• <b>hostAndPort</b>: Address used for replication between KV Store members and for accessing members from <code>splunkd</code>. Can be configured in <code>server.conf</code>.</li> </ul>
<i>members</i>	<p>For KV Store members, lists the following indicators.</p> <ul style="list-style-type: none"> <li>• <b>configVersion</b>: Version number that increases each time the KV Store cluster is updated.</li> <li>• <b>electionDate</b>: DateTime for election.</li> <li>• <b>electionDateSec</b>: Unix equivalent of <code>electionDate</code></li> <li>• <b>hostAndPort</b>: Address used for replication between KV Store members and for accessing members from <code>splunkd</code>. Can be configured in <code>server.conf</code>.</li> <li>• <b>lastHeartbeat</b>: Last time the requesting member sent a heartbeat to this member.</li> <li>• <b>lastHeartbeatRecv</b>: Last time this member replied on heartbeat.</li> <li>• <b>lastHeartbeatRecvSec</b>: Unix equivalent of <code>lastHeartbeatRecv</code></li> <li>• <b>lastHeartbeatSec</b>: Unix equivalent of <code>lastHeartbeat</code></li> <li>• <b>optimeDate</b>: Last recorded timestamp for this member in the operations log.</li> <li>• <b>optimeDateSec</b>: Unix equivalent of <code>optimeDate</code></li> <li>• <b>pingMs</b>: Latency (milliseconds for round trip).</li> <li>• <b>replicationStatus</b>: In standalone mode, this is KV Store captain. Otherwise, one of the following values. <ul style="list-style-type: none"> <li>◆ Startup</li> <li>◆ KV Store captain</li> <li>◆ Non-captain KV Store member</li> <li>◆ Recovering</li> <li>◆ Initial Sync</li> <li>◆ Unknown status</li> </ul> </li> </ul>

Name	Description
	<ul style="list-style-type: none"> <li>◆ Down</li> <li>◆ Rollback</li> <li>◆ Removed</li> <li>• uptime: Number of seconds this member has been online.</li> </ul>

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

```

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

```

---

## shcluster/captain/kvmigrate/start

<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
<i>storageEngine</i>	String	<b>Required.</b> Name of target storage engine, <i>wiredTiger</i> or <i>mmap</i> .
<i>isDryRun</i>	Boolean	Type <i>true</i> to complete pre-flight checks and exit without migrating. Setting is <i>false</i> by default.
<i>maxRetries</i>	Number	Number of times to retry a failed migration, per member.
<i>clusterPerc</i>	Number	Percentage of peers to migrate.
<i>peersList</i>	String	Names of peers to migrate.

### 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

`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
<i>clusterPerc</i>	Percentage of cluster members that have completed migration.

Name	Description
<i>migrationID</i>	ID number for the migration.
<i>migrationStartTime</i>	Timestamp that the migration began.
<i>peerRetryCount</i>	Number of times that the peer failed to migrate and retried.
<i>status</i>	Status of the migration.
<i>storageEngine</i>	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>
  </s:dict>
</s:key>
```

---

### shcluster/captain/kvmigrate/stop

```
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 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
<i>disabled</i>	Boolean indicating collection state. By default, the value is <code>false</code> , indicating that the collection is enabled.
<i>profilingEnabled</i>	Boolean indicating profiling status of slow-running operations. By default, this value is <code>false</code> , meaning that profiling is disabled.
<i>profilingThresholdMs</i>	Threshold for logging slow-running operations, in milliseconds. Applies only if <i>profilingEnabled</i> is <code>true</code> .

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

```

    <s:key name="profilingThresholdMs">100</s:key>
  </s:dict>
</content>
</entry>

```

## POST

Create a collection.

### Request parameters

Name	Type	Description
<i>name</i>	String	<b>Required.</b> Collection name
<i>profilingEnabled</i>	Boolean	A <code>collections.conf</code> file property that affects <i>profilingThresholdMs</i> . Defaults to <code>false</code> . Enable profiling of slow-running operations by setting <i>profilingEnabled</i> to <code>true</code> .
<i>profilingThresholdMs</i>	Number	Threshold for logging slow-running operations, in milliseconds. Applies only if <i>profilingEnabled</i> is <code>true</code> . Defaults to <code>100</code> . Set to <code>0</code> to log all slow-running operations.

### Returned values

Name	Description
<i>disabled</i>	Boolean indicating collection state. By default, the value is <code>false</code> , indicating that the collection is enabled.
<i>profilingEnabled</i>	Profiling status of slow-running operations, <i>profilingThresholdMs</i> . Defaults to <code>false</code> .
<i>profilingThresholdMs</i>	Threshold for logging slow-running operations, in milliseconds. Applies only if <i>profilingEnabled</i> is <code>true</code> .

### 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
<i>disabled</i>	Boolean indicating collection state. By default, the value is 0, meaning that the collection is enabled.
<i>field.&lt;fieldType&gt;</i>	Field type. One of the following values. <ul style="list-style-type: none"> <li>• array</li> <li>• number</li> <li>• bool</li> <li>• string</li> <li>• cidr</li> <li>• time</li> </ul>
<i>accelerated_fields.&lt;field_name&gt;</i>	Field acceleration name and JSON definition.
<i>enforceTypes</i>	Boolean indicating if data types are enforced when inserting data into the collection. Defaults to <i>false</i> .
<i>profilingEnabled</i>	Profiling status of slow-running operations, affecting <i>profilingThresholdMs</i> . By default, the value is <i>false</i> , meaning that profiling is disabled. If <i>true</i> , profiling is enabled.
<i>profilingThresholdMs</i>	Threshold for logging slow-running operations, in milliseconds. Applies only if <i>profilingEnabled</i> is <i>true</i> .
<i>replicate</i>	Boolean indicating whether the collection is replicated on indexers. Defaults to <i>false</i> , 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 <i>local=true</i> , local lookups will still be available.  When <i>true</i> , this collection is replicated on indexers.
<i>replication_dump_maximum_file_size</i>	Indicates the maximum file size (in KB) for each dump file when <i>replication_dump_strategy=auto</i> . Defaults to 10240KB.  If this value is larger than <i>concerningReplicatedFileSize</i> , which is set in the <i>distsearch.conf</i> file, the value of <i>concerningReplicatedFileSize</i> 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 <i>max_rows_in_memory_per_dump</i> setting in the <i>limits.conf</i> file.
<i>replication_dump_strategy</i>	One of the following two values.

Name	Description
	<ul style="list-style-type: none"> <li>• <code>auto</code>: Default. Dumps are stored in multiple files when the size of the collection exceeds the value of <code>replication_dump_maximum_file_size</code>.</li> <li>• <code>one_file</code>: Dump files are stored in a single file.</li> </ul>

## Example request and response

### XML Request

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/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
<i>field.&lt;fieldType&gt;</i>	String	Field type. One of the following values. <ul style="list-style-type: none"> <li>• array</li> <li>• number</li> <li>• bool</li> <li>• string</li> <li>• cidr</li> <li>• time</li> </ul>
<i>accelerated_fields.&lt;field_name&gt;</i>	String, JSON (see description)	The name of a field acceleration (string) and its definition, in JSON key value format. For example, <code>accelerated_fields.my_accel = {"id": 1}</code>

## Returned values

Name	Description
<i>disabled</i>	Collection state: <code>true</code> = disabled. <code>false</code> = [Default] enabled.
<i>field.&lt;fieldType&gt;</i>	Field type. One of the following values. <ul style="list-style-type: none"> <li>• array</li> <li>• number</li> <li>• bool</li> <li>• string</li> <li>• cidr</li> <li>• time</li> </ul>
<i>accelerated_fields.&lt;field_name&gt;</i>	The name of a field acceleration (string) and its definition, in JSON key value format. For example, <code>accelerated_fields.my_accel = {"id": 1}</code>
<i>profilingEnabled</i>	Profiling status of slow-running operations, affecting <i>profilingThresholdMs</i> . By default, the value is <code>false</code> , meaning that profiling is disabled. If <code>true</code> , profiling is enabled.
<i>profilingThresholdMs</i>	Threshold for logging slow-running operations, in milliseconds. Applies only if <i>profilingEnabled</i> is <code>true</code> .
<i>replicate</i>	Boolean indicating whether the collection is replicated on indexers. Defaults to <code>false</code> , 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 <code>local=true</code> , local lookups will still be available.  When <code>true</code> , this collection is replicated on indexers.
<i>replication_dump_maximum_file_size</i>	Indicates the maximum file size (in KB) for each dump file when <i>replication_dump_strategy</i> = <code>auto</code> . Defaults to 10240KB.  If this value is larger than <code>concerningReplicatedFileSize</code> , which is set in the <code>distsearch.conf</code> file, the value of <code>concerningReplicatedFileSize</code> 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 <code>max_rows_in_memory_per_dump</code> setting in the <code>limits.conf</code> file.
<i>replication_dump_strategy</i>	One of the following two values. <ul style="list-style-type: none"> <li>• <code>auto</code>: Default. Dumps are stored in multiple files when the size of the collection exceeds the value of <i>replication_dump_maximum_file_size</i>.</li> <li>• <code>one_file</code>: Dump files are stored in a single file.</li> </ul>

## 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
<i>query</i>	JSON object	Query JSON object. Conditional operators: <code>\$gt</code> , <code>\$gte</code> , <code>\$lt</code> , <code>\$lte</code> , and <code>\$ne</code> Logical operators: <code>\$and</code> , <code>\$or</code> , and <code>\$not</code> (invert conditional operators) Examples: <code>query={"title":"Item"}</code> (Select all documents with property <code>title</code> that has value <code>Item</code> ) <code>query={"price":{"\$gt":5}}</code> (Select all documents with <code>price</code> 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
<i>fields</i>	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 <code>_key</code> field. Examples: <code>fields=firstname,surname</code> (Include only <code>firstname</code> , <code>surname</code> , and <code>_key</code> fields) <code>fields=firstname,surname,_key:0</code> (Include only the <code>firstname</code> and <code>surname</code> fields. <code>fields=address:0</code> (Include all fields except the <code>address</code> field)
<i>limit</i>	Number	Maximum number of items to return. For example, to return five items, use <code>limit=5</code> .
<i>skip</i>	Number	Number of items to skip from the start. For example, to skip the first ten items, use <code>skip=10</code> .

Name	Type	Description
<i>sort</i>	String	Sort order. Examples: <code>sort=surname</code> (Sort by surname, ascending) <code>sort=surname,firstname</code> (Sort by surname, ascending, after firstname, ascending) <code>sort=surname:-1,firstname:1</code> (Sort by surname, descending, after firstname, ascending) <code>sort=surname:1,first name</code> (Sort by surname, ascending, after firstname, ascending)
<i>query</i>	JSON object	Query JSON object. Conditional operators: <code>\$gt</code> , <code>\$gte</code> , <code>\$lt</code> , <code>\$lte</code> , and <code>\$ne</code> Logical operators: <code>\$and</code> , <code>\$or</code> , and <code>\$not</code> (invert conditional operators) Examples: <code>query={"title": "Item"}</code> (Select all documents with property <code>title</code> that has value <code>Item</code> ) <code>query={"price":{"\$gt":5}}</code> (Select all documents with <code>price</code> 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/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/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\_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": "AAAAAAA" }, { "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 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, license endpoints are not applicable to Splunk Cloud deployments.

See Using the REST API in Splunk Cloud in the *Splunk REST API Tutorials* for more information.

---

## licenser/groups

`https://<host>:<mPort>/services/licenser/groups`

Provides access to the configuration of licensor groups.

A licensor group contains one or more licensor stacks that can operate concurrently. Only one licensor group is active at any given time.

### GET

Lists all licensor groups.

## Request parameters

Pagination and filtering parameters can be used with this method.

## Returned values

Name	Description
<i>is_active</i>	Indicates if the license group is active.
<i>stack_ids</i>	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
<i>is_active</i>	Indicates if the license group is active.
<i>stack_ids</i>	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
<i>is_active</i>	Boolean		<b>Required.</b> 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
------	-------------

<i>creation_time</i>	The creation time of this license, in Coordinated Universal Time (UTC).
<i>expiration_time</i>	The time this license expires, in Coordinated Universal Time (UTC).
<i>features</i>	The list of features and components enabled by this license.
<i>group_id</i>	The ID of the group to which this license belongs.
<i>label</i>	Plain text description of this license.
<i>license_hash</i>	Unique identifier for the license. The REST API uses this identifier to access this license.
<i>max_violations</i>	The maximum number of violations allowed during the specified window period ( <i>window_period</i> ). Searching is disabled when <i>max_violations</i> is exceeded.
<i>quota</i>	Daily indexing quota, in bytes, for this license.
<i>sourcetypes</i>	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.
<i>stack_id</i>	The ID of the license stack to which this license belongs.
<i>status</i>	The status of a license can be either VALID or EXPIRED.
<i>type</i>	Provides any additional information about the type of this license.
<i>window_period</i>	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
<i>name</i>	string		<b>Required.</b> Path to license file on server. If the payload parameter is specified, the name parameter is ignored.
<i>payload</i>	string		String representation of license, encoded in xml

### Returned values

Name	Description
<i>creation_time</i>	The creation time of this license, in Coordinated Universal Time (UTC).
<i>expiration_time</i>	The time this license expires, in Coordinated Universal Time (UTC).
<i>features</i>	The list of features and components enabled by this license.
<i>group_id</i>	The ID of the group to which this license belongs.
<i>label</i>	Plain text description of this license.
<i>license_hash</i>	Unique identifier for the license. The REST API uses this identifier to access this license.
<i>max_violations</i>	The maximum number of violations allowed during the specified window period ( <i>window_period</i> ). Searching is disabled when <i>max_violations</i> is exceeded.
<i>payload</i>	String representation of license, encoded in xml.
<i>quota</i>	Daily indexing quota, in bytes, for this license.
<i>sourcetypes</i>	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.
<i>stack_id</i>	The ID of the license stack to which this license belongs.
<i>status</i>	The status of a license can be either VALID or EXPIRED.
<i>type</i>	Provides any additional information about the type of this license.
<i>window_period</i>	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
<i>creation_time</i>	The creation time of this license, in Coordinated Universal Time (UTC).
<i>expiration_time</i>	The time this license expires, in Coordinated Universal Time (UTC).
<i>features</i>	The list of features and components enabled by this license.
<i>group_id</i>	The ID of the group to which this license belongs.
<i>label</i>	Plain text description of this license.
<i>license_hash</i>	Unique identifier for the license. The REST API uses this identifier to access this license.
<i>max_violations</i>	The maximum number of violations allowed during the specified window period ( <i>window_period</i> ). Searching is disabled when <i>max_violations</i> is exceeded.
<i>quota</i>	Daily indexing quota, in bytes, for this license.
<i>sourcetypes</i>	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.
<i>stack_id</i>	The ID of the license stack to which this license belongs.
<i>status</i>	The status of a license can be either VALID or EXPIRED.
<i>type</i>	Provides any additional information about the type of this license.
<i>window_period</i>	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
<i>add_ons</i>	List of add-ons resident on this instance, and add-on parameters.
<i>connection_timeout</i>	Instance connection timeout (seconds).
<i>features</i>	List of key-value pairs of the following features and their ENABLED/DISABLED status: <ul style="list-style-type: none"><li>• Acceleration</li><li>• AdvancedSearchCommands</li><li>• AdvancedXML</li><li>• Alerting</li><li>• AllowDuplicateKeys</li><li>• Auth</li><li>• CanBeRemoteManager</li><li>• CustomRoles</li><li>• DeployClient</li><li>• DeployServer</li><li>• DistSearch</li><li>• FwdData</li><li>• GuestPass</li><li>• KVStore</li><li>• LDAPAuth</li><li>• LocalSearch</li><li>• MultisiteClustering</li><li>• NontableLookups</li><li>• RcvData</li><li>• RcvSearch</li><li>• ResetWarnings"&gt;DISABLED_DUE_TO_LICENSE&lt;/s:key&gt;</li><li>• RollingWindowAlerts</li><li>• ScheduledAlerts</li><li>• ScheduledReports</li><li>• ScheduledSearch</li><li>• SearchheadPooling</li><li>• SigningProcessor</li><li>• SplunkWeb</li><li>• SyslogOutputProcessor</li><li>• UnisiteClustering</li></ul>
<i>last_manager_contact_attempt_time</i>	Time of last attempt to contact manager.
<i>last_manager_contact_success_time</i>	Time of last successful attempt to contact manager.

Name	Description
<i>last_trackerdb_service_time</i>	Time of last license servicing, tracking persistent store.
<i>license_keys</i>	List of license keys this instance is using.
<i>manager_guid</i>	Manager license GUID.
<i>manager_uri</i>	Manager license URI.
<i>receive_timeout</i>	Network layer receive timeout for communication to manager (seconds).
<i>send_timeout</i>	Network layer send timeout for communication to manager (seconds).
<i>peer_id</i>	This instance GUID.
<i>peer_label</i>	This instance server name.
<i>squash_threshold</i>	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:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
...
```



```

        </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
<i>category</i>	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
<i>create_time</i>	The time the message was created in the system, expressed in Coordinated Universal time (UTC).
<i>description</i>	The actual licenser message that is displayed.
<i>pool_id</i>	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.
<i>severity</i>	Indicates the severity of the message. The severity can be any of the following:  INFO  WARN  ERROR

Name	Description
<i>peer_id</i>	The ID of the license peer to which the message applies.
<i>stack_id</i>	The ID of the license stack to which the message applies. If a stack ID is not present, 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
<i>category</i>	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
<i>create_time</i>	The time the message was created in the system, expressed in Coordinated Universal time (UTC).
<i>description</i>	The actual licenser message that is displayed.
<i>pool_id</i>	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.
<i>severity</i>	Indicates the severity of the message. The severity can be any of the following:  INFO  WARN  ERROR
<i>peer_id</i>	The ID of the license peer to which the message applies.
<i>stack_id</i>	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
<i>description</i>	Description of the license pool.
<i>quota</i>	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.
<i>peers</i>	peerids that are members of this pool.  Returned as a list in Atom format. See example below.
<i>peers_usage_bytes</i>	Usage, in bytes, of peers to this license.
<i>stack_id</i>	Stack ID of the stack corresponding to this pool.
<i>used_bytes</i>	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

<i>description</i>	String		Description of this pool
Name	Type	Default	Description
<i>name</i>	String		<b>Required.</b> The name of the license pool you are creating.
<i>quota</i>	String		<b>Required.</b> 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.
<i>peers</i>	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.
<i>stack_id</i>	Enum		<b>Required.</b> 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
<i>description</i>	Description of the license pool.
<i>quota</i>	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.
<i>peers</i>	peerids that are members of this pool.  Returned as a list in Atom format. See example below.
<i>peers_usage_bytes</i>	Usage, in bytes, of peers to this license.
<i>stack_id</i>	Stack ID of the stack corresponding to this pool.
<i>used_bytes</i>	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
<i>append_peers</i>	Boolean		Flag which controls whether newly specified peers is appended to existing peers list or overwritten
<i>description</i>	String		Description of this pool
<i>quota</i>	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.
<i>peers</i>	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
<i>label</i>	Plain text name for the license peer.
<i>pool_ids</i>	License pools for which this license peer is a member.
<i>stack_ids</i>	License stacks for which this license peer is a member.
<i>warning_count</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
</opensearch:startIndex>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:totalResults>1</opensearch:totalResults>
</author>
</generator>
</updated>
</id>
</title>
```

```

        </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
<i>label</i>	Plain text name for the license peer.
<i>pool_ids</i>	License pools for which this license peer is a member.
<i>stack_ids</i>	License stacks for which this license peer is a member.
<i>warning_count</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
</search>
```



```

        </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
<i>label</i>	The name of this license stack.
<i>quota</i>	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
<i>type</i>	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>
```

```

    </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
<i>label</i>	The name of this license stack.
<i>quota</i>	The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the license stack.
<i>type</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
</stacks>
```

```

        </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.

### GET

Enumerate license usage information from the last minute.

### Request parameters

Pagination and filtering parameters can be used with this method.

### Returned values

Name	Description
<i>quota</i>	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.
<i>peers_usage_bytes</i>	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 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 *Splunk REST API Tutorials* 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
<i>earliest</i>	String	Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is <code>-1d</code> .
<i>filter</i>	String	Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as <code>index</code> or <code>dimension</code> . For example, to specify a dimension named <code>os</code> , use <code>filter=os</code> . To specify two index names and values such as <code>index=index1</code> and <code>index=index2</code> , use <code>index%3dindex1%26index%3dindex2</code> .
<i>latest</i>	String	Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is <code>now</code> .
<i>metric_name</i>	String	<b>Required.</b> 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.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
<i>earliest</i>	String	Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is <code>-1d</code> .
<i>filter</i>	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 <code>os</code> , use <code>filter=os</code> . To specify two index names and values such as <code>index=index1</code> and <code>index=index2</code> , use <code>index%3dindex1%26index%3dindex2</code> .
<i>latest</i>	String	Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is <code>now</code> .
<i>metric_name</i>	String	<b>Required.</b> 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
<i>name</i>	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.
<i>summaries</i>	<p>A comma-separated list of the rollup summaries associated with the source metric index. Each summary configuration consists of a <code>span</code> and a <code>rollup_index</code>. The <code>span</code> is the interval by which the search head generates the aggregated rollup metric data points that make up the summary. The <code>rollup_index</code> is the target index for the rollup summary. The endpoint uses the following format when it lists summaries:</p> <p>&lt;span_1&gt; &lt;rollup_index_1&gt;,&lt;span_2&gt; &lt;rollup_index_2&gt;...&lt;span_n&gt; &lt;rollup_index_n&gt;</p>

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

```

    <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>
</s:key>
</s:dict>
</content>
</entry>
</feed>

```

**POST**

Creates rollup policies for a specified metric index.

### Request parameters

Name	Type	Description
<i>name</i>	String	<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.
<i>summaries</i>	String	<b>Required.</b> Specify one or more rollup summaries, separated by commas. A rollup summary is a combination of a rollup metric index and a rollup period. The rollup period is the <i>span</i> . 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 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>. Defaults to 1hr <name>.
<i>default_agg</i>	String	<b>Optional.</b> 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 <i>defaultAggregation</i> can be overruled for specific metrics by the <i>aggregation.&lt;metric_name&gt;</i> setting. This setting supports the following functions: avg, count, max, median, min, perc<int>, and sum. Defaults to avg.
<i>metric_list</i>	String	<b>Optional.</b> A comma-separated list of metric names. All of the listed metrics must appear in the source metric index identified by the <i>name</i> parameter. This list works in conjunction with the <i>metric_list_type</i> parameter to create a filter at the search head that allows certain metrics to be rolled up but not others. Defaults to empty string.
<i>metric_list_type</i>	[included   excluded]	<b>Optional.</b> Works in conjunction with the <i>metric_list</i> 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 <i>excluded</i> .

Name	Type	Description
		<ul style="list-style-type: none"> <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>
<code>dimension_list</code>	String	<b>Optional.</b> 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.
<code>dimension_list_type</code>	[included   excluded]	<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. Defaults to <code>excluded</code> . <ul style="list-style-type: none"> <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>
<code>metric_overrides</code>	String	<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 # characters. Each metric override uses the following syntax: <code>&lt;metric_name&gt; &lt;aggregation_function_1&gt;#&lt;aggregation_function_2&gt;#â &lt;aggregation_function_3&gt;</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.
<code>disabled</code>	Specifies whether the metric rollup policy is disabled.	
<code>eai:appName</code>	The Splunk app for which the metric rollup policy is defined. For example, the search app.	

## Returned values

Name	Description
<code>aggregation.&lt;metric_name&gt;</code>	Overrides the default aggregation or set of aggregations for the specified <code>metric_name</code> and gives it a different aggregation or set of aggregations instead. Defined by the <code>metric_overrides</code> argument.
<code>defaultAggregation</code>	The default aggregation methods for the rollup policy, separated by # characters.
<code>dimensionList</code>	Comma-separated list of dimensions to be included or excluded from the aggregations, depending on the value of <code>dimensionListType</code> .
<code>dimensionListType</code>	Indicates whether the <code>dimensionList</code> should be <code>included</code> or <code>excluded</code> from the rollup policy.
<code>metricList</code>	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 <code>dimensionListType</code>



Name	Description
<i>metricListType</i>	Indicates whether the <code>metricList</code> should be included or excluded from the rollup policy.
<i>rollup.&lt;summary number&gt;.rollupIndex</i>	The target rollup index for a specific summary. Summaries are identified by the <code>&lt;summary number&gt;</code> .
<i>rollup.&lt;summary number&gt;.span</i>	The rollup span for a specific summary. Summaries are identified by the <code>&lt;summary number&gt;</code> .

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

```

    <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
<i>summaries</i>	<p>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:</p> <p>&lt;span_1&gt; &lt;rollup_index_1&gt;,&lt;span_2&gt; &lt;rollup_index_2&gt;...&lt;span_n&gt; &lt;rollup_index _n&gt;</p>

## 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>
</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
<i>default_agg</i>	String	<b>Optional.</b> 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 <code>defaultAggregation</code> can be overruled for specific metrics by the <code>aggregation.&lt;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> .
<i>metric_list</i>	String	<b>Optional.</b> 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.

Name	Type	Description
<i>metric_list_type</i>	[included   excluded]	<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 style="list-style-type: none"> <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>
<i>dimension_list</i>	string	<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.
<i>dimension_list_type</i>	[included   excluded]	<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 style="list-style-type: none"> <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>
<i>metric_overrides</i>	String	<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 # characters. Each metric override uses the following syntax: <code>&lt;metric_name&gt; &lt;aggregation_function_1&gt;#&lt;aggregation_function_2&gt;#â &lt;aggregation_function_3&gt;</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.
<i>summaries</i>	string	<b>Optional.</b> Specify one or more rollup summaries, separated by commas. A rollup summary is a combination of a rollup metric index and a rollup period. 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. 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; &lt;rollup_index_1&gt;,&lt;span_2&gt; &lt;rollup_index_2&gt;...&lt;span_n&gt; &lt;rollup_index_n&gt;</code>

## Returned values

Name	Description
<i>aggregation.&lt;metric_name&gt;</i>	Overrides the default aggregation or set of aggregations for the specified <code>metric_name</code> and gives it a different aggregation or set of aggregations instead. Defined by the <code>metric_overrides</code> argument.
<i>defaultAggregation</i>	The default aggregation methods for the rollup policy, separated by # characters.
<i>dimensionList</i>	Comma-separated list of dimensions to be included or excluded from the aggregations, depending on the value of <code>dimensionListType</code> .
<i>dimensionListType</i>	Indicates whether the <code>dimensionList</code> should be <code>included</code> or <code>excluded</code> from the rollup policy.
<i>metricList</i>	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 <code>dimensionListType</code> .
<i>metricListType</i>	Indicates whether the <code>metricList</code> should be <code>included</code> or <code>excluded</code> from the rollup policy.
<i>rollup.&lt;summary number&gt;.rollupIndex</i>	The target rollup index for a specific summary. Summaries are identified by the <code>&lt;summary number&gt;</code> .
<i>rollup.&lt;summary number&gt;.span</i>	The rollup span for a specific summary. Summaries are identified by the <code>&lt;summary number&gt;</code> .

## 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 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, output endpoints are not applicable to Splunk Cloud deployments.

See Using the REST API in Splunk Cloud in the the *Splunk REST API Tutorials* 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
<i>autoLB</i>	Specifies whether Auto Load balance method is used.
<i>defaultGroup</i>	Target group names. The forwarder sends all data to the specified groups. Starting with 4.2, this attribute is no longer required.
<i>disabled</i>	Indicates if tcpout settings are disabled.
<i>forwardedindex.0.whitelist</i>	Specifies 0th whitelist filter. <i>forwardedindex.&lt;n&gt;.whitelist</i> decides which events get forwarded based on the indexes they belong to.
<i>forwardedindex.1.blacklist</i>	Specifies 1st blacklist filter. <i>forwardedindex.&lt;n&gt;.blacklist</i> specifies index for which events are not forwarded.
<i>forwardedindex.2.whitelist</i>	Specifies 2nd whitelist filter. <i>forwardedindex.&lt;n&gt;.whitelist</i> decides which events get forwarded based on the indexes they belong to.
<i>forwardedindex.filter.disable</i>	Specifies whether filtering of forwarded data based on index is disabled.
<i>indexAndForward</i>	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.
<i>maxQueueSize</i>	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 parameter 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
<i>defaultGroup</i>	String		<p>Comma-separated list of one or more target group names, specified later in [tcpout:&lt;target_group&gt;] stanzas of outputs.conf.spec file.</p> <p>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 <code>_TCP_ROUTING</code> setting, which in turn can be overridden by a props.conf/transforms.conf modifier.</p> <p>Starting with 4.2, this attribute is no longer required.</p>
<i>disabled</i>	Boolean		Disables default tcpout settings

Name	Type	Default	Description
<i>dropEventsOnQueueFull</i>	Number		<p>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).</p> <p>CAUTION: Do not set this value to a positive integer if you are monitoring files.</p> <p>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.</p> <p>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.</p>
<i>heartbeatFrequency</i>	Number		<p>How often (in seconds) to send a heartbeat packet to the receiving server.</p> <p>Heartbeats are only sent if <code>sendCookedData=true</code>. Defaults to 30 seconds.</p>
<i>indexAndForward</i>	Boolean		<p>Specifies whether to index all data locally, in addition to forwarding it. Defaults to false.</p> <p>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 <code>outputs.conf</code>. It cannot be overridden in a target group.</p>
<i>maxQueueSize</i>	Number		<p>Specify an integer or integer[KB MB GB].</p> <p>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 (<code>useACK=true</code>).</p> <p>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.</p> <p>For heavy forwarders sending parsed data, <code>maxQueueSize</code> 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.</p> <p>If specified as a lone integer (for example, <code>maxQueueSize=100</code>), <code>maxQueueSize</code> 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, <code>maxQueueSize</code> is the maximum number of data blocks.</p> <p>If specified as an integer followed by KB, MB, or GB (for example, <code>maxQueueSize=100MB</code>), <code>maxQueueSize</code> 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).</p>
<i>name</i> required	String		Configuration to be edited. The only valid value is "tcpout".

Name	Type	Default	Description
<i>sendCookedData</i>	Boolean		<p>If true, events are cooked (processed by Splunk software). If false, events are raw and untouched prior to sending. Defaults to true.</p> <p>Set to false if you are sending to a third-party system.</p>

### 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
<i>defaultGroup</i>	String		<p>Comma-separated list of one or more target group names, specified later in [tcpout:&lt;target_group&gt;] stanzas of outputs.conf.spec file.</p> <p>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.</p> <p>Starting with 4.2, this attribute is no longer required.</p>

Name	Type	Default	Description
<i>disabled</i>	Boolean		Disables default tcpout settings
<i>dropEventsOnQueueFull</i>	Number		<p>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).</p> <p><b>Caution:</b> Do not set this value to a positive integer if you are monitoring files.</p> <p>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.</p> <p>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.</p>
<i>heartbeatFrequency</i>	Number		<p>How often (in seconds) to send a heartbeat packet to the receiving server.</p> <p>Heartbeats are only sent if <code>sendCookedData=true</code>. Defaults to 30 seconds.</p>
<i>indexAndForward</i>	Boolean		<p>Specifies whether to index all data locally, in addition to forwarding it. Defaults to false.</p> <p>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 <code>outputs.conf</code>. It cannot be overridden in a target group.</p>
<i>maxQueueSize</i>	Number		<p>Specify an integer or integer[KB MB GB].</p> <p>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 (<code>useACK=true</code>).</p> <p>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.</p> <p>For heavy forwarders sending parsed data, <code>maxQueueSize</code> 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.</p> <p>If specified as a lone integer (for example, <code>maxQueueSize=100</code>), <code>maxQueueSize</code> 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, <code>maxQueueSize</code> is the maximum number of data blocks.</p> <p>If specified as an integer followed by KB, MB, or GB (for example, <code>maxQueueSize=100MB</code>), <code>maxQueueSize</code> 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).</p>

Name	Type	Default	Description
<i>sendCookedData</i>	Boolean		<p>If true, events are cooked (processed by Splunk software). If false, events are raw and untouched prior to sending. Defaults to true.</p> <p>Set to false if you are sending to a third-party system.</p>

#### 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
<i>disabled</i>	Indicates if tcpout is disabled for this group.
<i>method</i>	Specifies the type of output processor. Valid values: (tcpout   syslog)
<i>servers</i>	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>
...
```

</content>  
</entry>

POST

Configure a group of one or more data forwarding destinations.

Request parameters

Name	Type	Default	Description
<i>compressed</i>	Boolean	false	If true, forwarder sends compressed data.  If set to true, the receiver port must also have compression turned on.
<i>disabled</i>	Boolean	false	If true, disables the group.
<i>dropEventsOnQueueFull</i>	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).  <b>Caution:</b> 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.
<i>heartbeatFrequency</i>	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.
<i>maxQueueSize</i>	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.

Name	Type	Default	Description
			<p>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.</p> <p>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).</p>
<i>method</i>	Enum		<p>Valid values: (tcpout   syslog)</p> <p>Specifies the type of output processor.</p>
<i>name required</i>	String		The name of the group of receivers.
<i>sendCookedData</i>	Boolean	true	<p>If true, send cooked events (events processed by Splunk software).</p> <p>If false, events are raw and untouched prior to sending. Set to false if you are sending to a third-party system.</p> <p>Defaults to true.</p>
<i>servers required</i>	String		Comma-separated list of servers to include in the group.
<i>token</i>	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
<i>autoLB</i>	Indicates if the forwarder performs automatic load balancing.  See the description for the autoLB parameter in POST data/outputs/tcp/group for details.
<i>disabled</i>	Indicates if tcpout is disabled for this group.
<i>method</i>	Specifies the type of output processor.  Valid values: (tcpout   syslog)
<i>servers</i>	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>maxPersistentQueueSizeInMega</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
<i>compressed</i>	Boolean	false	<p>If true, forwarder sends compressed data.</p> <p>If set to true, the receiver port must also have compression turned on.</p>

Name	Type	Default	Description
<i>disabled</i>	Boolean	false	If true, disables the group.
<i>dropEventsOnQueueFull</i>	Number	-1	<p>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).</p> <p><b>Caution:</b> Do not set this value to a positive integer if you are monitoring files.</p> <p>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.</p> <p>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.</p>
<i>heartbeatFrequency</i>	Number	30	<p>How often (in seconds) to send a heartbeat packet to the group.</p> <p>Heartbeats are only sent if <code>sendCookedData=true</code>. Defaults to 30 seconds.</p>
<i>maxQueueSize</i>	Number	auto	<p>Specify either an integer or integer[KB MB GB].</p> <p>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 (<code>useACK=true</code>).</p> <p>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.</p> <p>For heavy forwarders sending parsed data, <code>maxQueueSize</code> 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.</p> <p>If specified as a lone integer (for example, <code>maxQueueSize=100</code>), <code>maxQueueSize</code> 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, <code>maxQueueSize</code> is the maximum number of data blocks.</p> <p>If specified as an integer followed by KB, MB, or GB (for example, <code>maxQueueSize=100MB</code>), <code>maxQueueSize</code> 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).</p>
<i>method</i>	Enum		<p>Valid values: (tcpout   syslog)</p> <p>Specifies the type of output processor.</p>
<i>sendCookedData</i>	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.
<i>servers required</i>	String		Comma-separated list of servers to include in the group.
<i>token</i>	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
<i>destHost</i>	DNS name of the destination server.
<i>destIp</i>	IP address of the destination server.
<i>destPort</i>	Port on which the destination server is listening.
<i>disabled</i>	Indicates if the outputs to the destination server is disabled.
<i>method</i>	The data distribution method used when two or more servers exist in the same forwarder group. Valid values: (clone   balance   autobalance)
<i>sourcePort</i>	Port on destination server where data is forwarded.
<i>status</i>	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
<i>disabled</i>	Boolean		If true, disables the forwarder.
<i>method</i>	Enum		Valid values: (clone   balance   autobalance)  The data distribution method used when two or more servers exist in the same forwarder group.
<i>name required</i>	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.
<i>sslAltNameToCheck</i>	String		The alternate name to match in the remote server's SSL certificate.
<i>sslCertPath</i>	String		Path to the client certificate. If specified, connection uses SSL.
<i>sslCipher</i>	String		SSL Cipher in the form ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
<i>sslCommonNameToCheck</i>	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.
<i>sslPassword</i>	String		The password associated with the CAcert.  The default Splunk Enterprise CAcert uses the password "password."
<i>sslRootCAPath</i>	String		The path to the root certificate authority file (optional).
<i>sslVerifyServerCert</i>	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
<i>disabled</i>	Indicates if the outputs to the destination server is disabled.
<i>method</i>	<p>The data distribution method used when two or more servers exist in the same forwarder group.</p> <p>Valid values: (clone   balance   autobalance)</p>

## 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
------	------	---------	-------------

<i>disabled</i>	Boolean		If true, disables the forwarder.
<i>method</i>	Enum		Valid values: (clone   balance   autobalance)  The data distribution method used when two or more servers exist in the same forwarder group.
<i>sslAltNameToCheck</i>	String		The alternate name to match in the remote server's SSL certificate.
<i>sslCertPath</i>	String		Path to the client certificate. If specified, connection uses SSL.
<i>sslCipher</i>	String		SSL Cipher in the form ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
<i>sslCommonNameToCheck</i>	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.
<i>sslPassword</i>	String		The password associated with the CAcert.  The default Splunk Enterprise CAcert uses the password "password."
<i>sslRootCAPath</i>	String		The path to the root certificate authority file (optional).
<i>sslVerifyServerCert</i>	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
<i>destHost</i>	DNS name of the destination server.
<i>destIp</i>	IP address of the destination server.
<i>destPort</i>	Port on which the destination server is listening.
<i>sourcePort</i>	Port on destination server where data is forwarded.
<i>status</i>	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
<i>disabled</i>	Specifies whether global syslog configuration is disabled.
<i>server</i>	Specifies server:port where data is forwarded.
<i>type</i>	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
<i>disabled</i>	Boolean		If true, disables global syslog settings.
<i>name required</i>	String		Name of the syslog output group. This is name used when creating syslog configuration in <code>outputs.conf</code> .
<i>priority</i>	Number		Sets syslog priority value.  The priority value should specified as an integer. See <code>\$SPLUNK_HOME/etc/system/README/outputs.conf.spec</code> for details.
<i>server</i>	String		host:port of the server where syslog data should be sent

Name	Type	Default	Description
<i>syslogSourceType</i>	String		<p>Specifies a rule for handling data in addition to that provided by the "syslog" sourcetype. By default, there is no value for syslogSourceType.</p> <p>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.</p> <p>To match a source type explicitly, use the pattern "sourcetype::sourcetype_name." For example</p> <pre>syslogSourcetype = sourcetype::apache_common</pre> <p>Data that is "syslog" or matches this setting is assumed to already be in syslog format.</p> <p>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.</p>
<i>timestampformat</i>	String		<p>Format of timestamp to add at start of the events to be forwarded.</p> <p>The format is a strftime-style timestamp formatting string. See <a href="#">\$SPLUNK_HOME/etc/system/README/outputs.conf.spec</a> for details.</p>
<i>type</i>	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
<i>disabled</i>	Specifies whether global syslog configuration is disabled.
<i>server</i>	Specifies server:port where data is forwarded.
<i>type</i>	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
<i>disabled</i>	Boolean		If true, disables global syslog settings.
<i>priority</i>	Number		<p>Sets syslog priority value.</p> <p>The priority value should specified as an integer. See <code>\$SPLUNK_HOME/etc/system/README/outputs.conf.spec</code> for details.</p>
<i>server</i>	String		host:port of the server where syslog data should be sent
<i>syslogSourceType</i>	String		<p>Specifies a rule for handling data in addition to that provided by the "syslog" sourcetype. By default, there is no value for syslogSourceType.</p> <p>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.</p> <p>To match a source type explicitly, use the pattern "sourcetype::sourcetype_name." For example</p> <pre>syslogSourceType = sourcetype::apache_common</pre> <p>Data that is "syslog" or matches this setting is assumed to already be in syslog format.</p> <p>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.</p>
<i>timestampformat</i>	String		<p>Format of timestamp to add at start of the events to be forwarded.</p> <p>The format is a strftime-style timestamp formatting string. See <code>\$SPLUNK_HOME/etc/system/README/outputs.conf.spec</code> for details.</p>
<i>type</i>	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.
- Scheduled view objects.

## 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:dict>
  </content>
</entry>

```

```

<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](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
<i>triggered_alert_count</i>	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
<i>actions</i>	Any additional alert actions triggered by this alert.
<i>alert_type</i>	Indicates if the alert was historical or real-time.
<i>digest_mode</i>	
<i>expiration_time_rendered</i>	
<i>savedsearch_name</i>	Name of the saved search that triggered the alert.
<i>severity</i>	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.
<i>sid</i>	The search ID of the search that triggered the alert.
<i>trigger_time</i>	The time the alert was triggered.
<i>trigger_time_rendered</i>	
<i>triggered_alerts</i>	

## 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
<i>action.&lt;action_name&gt;</i>	Indicates whether the <action_name> is enabled or disabled for a particular metric alert. Valid values for action_name are: <ul style="list-style-type: none"><li>•email</li><li>•logevent</li><li>•rss</li><li>•script</li><li>•webhook</li></ul> For more information about the alert action options see the <code>alert_actions.conf</code> file.
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>	Overrides the setting defined for an action in the <code>alert_actions.conf</code> file with a new setting that is valid only for the metric alert configuration to which it is applied.
<i>condition</i>	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.

Name	Description
	Must reference at least one ' <code>&lt;mstats_aggregation&gt;(&lt;metric_name&gt;)</code> ' clause in single quotes. The condition can also reference dimensions specified in the <code>groupby</code> setting.
<i>description</i>	Description of the metric alert.
<i>filter</i>	Provides one or more Boolean expressions like <code>&lt;dimension_field&gt;=&lt;value&gt;</code> 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 <code>metric_indexes</code> setting to provide the complete search filter for the alert.
<i>groupby</i>	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.
<i>label.&lt;label-name&gt;</i>	Arbitrary key-value pairs for labeling this alert.
<i>metric_indexes</i>	Specifies one or more metric indexes, delimited by comma.  Combines with the <code>filter</code> setting to provide the complete search filter for the alert.
<i>splunk_ui.&lt;label-name&gt;</i>	An arbitrary key-value pair that is automatically generated by the Splunk software for its internal use only. Do not change it.
<i>trigger.expires</i>	Sets the period of time that a triggered alert record displays on the Triggered Alerts page.
<i>trigger.max_tracked</i>	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.
<i>trigger.suppress</i>	Specifies the suppression period to silence alert actions and notifications. <ul style="list-style-type: none"> <li>• The suppression period goes into effect when an alert is triggered.</li> <li>• During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out.</li> <li>• 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.</li> </ul>

## 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
<i>action.&lt;action-name&gt;</i>	Boolean	Indicates whether the <code>&lt;action_name&gt;</code> is enabled or disabled for a particular metric alert. Valid values for <code>action_name</code> are: <ul style="list-style-type: none"><li>• email</li><li>• logevent</li><li>• rss</li><li>• script</li><li>• webhook</li></ul> For more information about the alert action options see the <code>alert_actions.conf</code> file.
<i>action.&lt;action-name&gt;.&lt;parameter&gt;</i>	String	Override the global setting defined for an <code>&lt;action-name&gt;</code> in the <code>alert_actions.conf</code> file with a new setting that is valid only for the metric alert configuration to which it is applied.
<i>condition required</i>	Boolean eval expression	Specifies an alert condition for one or more <code>metric_name</code> 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 ' <code>&lt;mstats_aggregation&gt;(&lt;metric_name&gt;)</code> ' clause in single quotes. The condition can also reference dimensions specified in the <code>groupby</code> setting.
<i>description</i>	String	Provide a description of the streaming metric alert.
<i>filter</i>	String	Specify one or more Boolean expressions like <code>&lt;dimension_field&gt;=&lt;value&gt;</code> 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 <code>metric_indexes</code> setting to provide the complete search filter for the alert.
<i>groupby</i>	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.
<i>label.&lt;label-name&gt;</i>	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 <code>`alerts/metric_alerts`</code> endpoint.
<i>metric_indexes required</i>	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.
<i>name required</i>	String	Specify the name of the streaming metric alert.
<i>trigger.expires</i>	String	Set the period of time that a triggered alert record displays on the Triggered Alerts page.

Name	Type	Description
		<ul style="list-style-type: none"> <li>Use <code>&lt;positive integer&gt;&lt;time-unit&gt;</code>, where <code>&lt;time_unit&gt;</code> can be 'm' for minutes, 'h' for hours, and 'd' for days.</li> <li>Set to 0 to make triggered alerts expire immediately so they do not appear on the Triggered Alerts page at all.</li> </ul> <p>Default is 24h.</p>
<code>trigger.max_tracked</code>	Number	<p>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.</p> <p>Defaults to 20.</p>
<code>trigger.suppress</code>	String	<p>Define the suppression period to silence alert actions and notifications.</p> <ul style="list-style-type: none"> <li>The suppression period goes into effect when an alert is triggered.</li> <li>During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out.</li> <li>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.</li> </ul> <p>Use <code>&lt;number&gt;m</code> to specify a timespan in minutes. Default is 0m.</p>

## 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
<i>action.&lt;action_name&gt;</i>	<p>Indicates whether the <code>&lt;action_name&gt;</code> is enabled or disabled for a particular metric alert. Valid values for <code>action_name</code> are:</p> <ul style="list-style-type: none"><li>• email</li><li>• logevent</li><li>• rss</li><li>• script</li><li>• webhook</li></ul> <p>For more information about the alert action options see the <code>alert_actions.conf</code> file.</p>
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>	<p>Overrides the setting defined for an action in the <code>alert_actions.conf</code> file with a new setting that is valid only for the metric alert configuration to which it is applied.</p>
<i>condition</i>	<p>Specifies an alert condition for one or more <code>metric_name</code> 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.</p> <p>Must reference at least one '<code>&lt;mstats_aggregation&gt;(&lt;metric_name&gt;)</code>' clause in single quotes. The condition can also reference dimensions specified in the <code>groupby</code> setting.</p>
<i>description</i>	<p>Description of the metric alert.</p>
<i>groupby</i>	<p>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.</p>
<i>filter</i>	<p>Provides one or more Boolean expressions like <code>&lt;dimension_field&gt;=&lt;value&gt;</code> 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'.</p> <p>Combines with the <code>metric_indexes</code> setting to provide the complete search filter for the alert.</p>
<i>label.&lt;label-name&gt;</i>	<p>Arbitrary key-value pairs for labeling this alert.</p>
<i>metric_indexes</i>	<p>Specifies one or more metric indexes, delimited by comma.</p> <p>Combines with the <code>filter</code> setting to provide the complete search filter for the alert.</p>

Name	Description
<i>splunk_ui.&lt;label-name&gt;</i>	An arbitrary key-value pair that is automatically generated by the Splunk software for its internal use only. Do not change it.
<i>trigger.expires</i>	Sets the period of time that a triggered alert record displays on the Triggered Alerts page.
<i>trigger.max_tracked</i>	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.
<i>trigger.suppress</i>	<p>Specifies the suppression period to silence alert actions and notifications.</p> <ul style="list-style-type: none"> <li>• The suppression period goes into effect when an alert is triggered.</li> <li>• During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out.</li> <li>• 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.</li> </ul>

## 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:dict>
</content>
</entry>
</feed>

```

**POST**

Update the named streaming metric alert.

Request parameters

Name	Type	Description
<i>action.&lt;action-name&gt;</i>	Boolean	<p>Indicates whether the <i>&lt;action_name&gt;</i> is enabled or disabled for a particular metric alert. Valid values for <i>&lt;action_name&gt;</i> are:</p> <ul style="list-style-type: none"> <li>• email</li> <li>• logevent</li> <li>• rss</li> <li>• script</li> <li>• webhook</li> </ul> <p>For more information about the alert action options see the <i>alert_actions.conf</i> file.</p>
<i>action.&lt;action-name&gt;.&lt;parameter&gt;</i>	String	<p>Override the global setting defined for an <i>&lt;action-name&gt;</i> in the <i>alert_actions.conf</i> file with a new setting that is valid only for the metric alert configuration to which it is applied.</p>

Name	Type	Description
<i>condition required</i>	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 ' <code>&lt;mstats_aggregation&gt;(&lt;metric_name&gt;)</code> ' clause in single quotes. The condition can also reference dimensions specified in the <code>groupby</code> setting.
<i>description</i>	String	Provide a description of the streaming metric alert.
<i>groupby</i>	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.
<i>filter</i>	String	Specify one or more Boolean expressions like <code>&lt;dimension_field&gt;=&lt;value&gt;</code> 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 <code>metric_indexes</code> setting to provide the complete search filter for the alert.
<i>label.&lt;label-name&gt;</i>	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 <code>alerts/metric_alerts</code> endpoint.
<i>metric_indexes required</i>	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.
<i>trigger.expires</i>	String	Set the period of time that a triggered alert record displays on the Triggered Alerts page. <ul style="list-style-type: none"> <li>Use <code>&lt;positive integer&gt;&lt;time-unit&gt;</code>, where <code>&lt;time_unit&gt;</code> can be 'm' for minutes, 'h' for hours, and 'd' for days.</li> <li>Set to 0 to make triggered alerts expire immediately so they do not appear on the Triggered Alerts page at all.</li> </ul> Default is 24h.
<i>trigger.max_tracked</i>	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.
<i>trigger.suppress</i>	String	Define the suppression period to silence alert actions and notifications. <ul style="list-style-type: none"> <li>The suppression period goes into effect when an alert is triggered.</li> <li>During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out.</li> <li>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.</li> </ul> Use <code>&lt;number&gt;m</code> 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/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
<i>changes_colorder</i>	Indicates whether the script output should be used to change the column ordering of the fields.
<i>disabled</i>	Indicates if the command is disabled.
<i>enableheader</i>	<p>Indicate whether or not your script is expecting header information or not.</p> <p>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.</p> <p><i>Note:</i> Should be set to true if you use splunk.Intersplunk</p>
<i>filename</i>	<p>Name of script file for command.</p> <p>&lt;stanza-name&gt;.pl for perl.</p> <p>&lt;stanza-name&gt;.py for python.</p>
<i>generates_timeorder</i>	If generating = false and streaming = true, indicates if the command changes the order of events w/respect to time.
<i>generating</i>	Indicates if the command generates new events.
<i>maxinputs</i>	<p>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.</p> <p>0 indicates no limit. Defaults to 50000.</p>
<i>outputheader</i>	<p>If true, the output of script should be a header section + blank line + csv output.</p> <p>If false, script output should be pure csv only.</p>

Name	Description
<i>passauth</i>	If true, passes an authentication token on the start of input.
<i>required_fields</i>	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 <code>''</code> .
<i>requires_preop</i>	Indicates whether the command sequence specified by the <code>streaming_preop</code> key is required for proper execution or is it an optimization only.  Default is false ( <code>streaming_preop</code> not required).
<i>retainsevents</i>	Indicates whether the command retains events (the way the <code>sort/dedup/cluster</code> commands do) or whether the command transforms them (the way the <code>stats</code> command does).
<i>streaming</i>	Indicates whether the command is streamable.
<i>supports_getinfo</i>	Indicates whether the command supports dynamic probing for settings (first argument invoked == <code>__GETINFO__</code> or <code>__EXECUTE__</code> ).
<i>supports_rawargs</i>	Indicates whether the command supports raw arguments being passed to it or if it uses parsed arguments (where quotes are stripped).
<i>type</i>	Specifies the type of command. The only valid value for this attribute is <code>python</code> .

## 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:dict>
    </content>
  </entry>
</feed>
```

```

<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
<i>changes_colorder</i>	Indicates whether the script output should be used to change the column ordering of the fields.
<i>disabled</i>	Indicates if the command is disabled.
<i>enableheader</i>	<p>Indicate whether or not your script is expecting header information or not.</p> <p>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.</p> <p><i>Note:</i> Should be set to true if you use splunk.Intersplunk</p>
<i>filename</i>	<p>Name of script file for command.</p> <p>&lt;stanza-name&gt;.pl for perl.</p> <p>&lt;stanza-name&gt;.py for python.</p>

Name	Description
<i>generates_timeorder</i>	If generating = false and streaming = true, indicates if the command changes the order of events w/respect to time.
<i>generating</i>	Indicates if the command generates new events.
<i>maxinputs</i>	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.
<i>outputheader</i>	If true, the output of script should be a header section + blank line + csv output.  If false, script output should be pure csv only.
<i>passauth</i>	If true, passes an authentication token on the start of input.
<i>required_fields</i>	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 '*'.  
<i>requires_preop</i>	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 (streaming_preop not required).
<i>retainsevents</i>	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).
<i>streaming</i>	Indicates whether the command is streamable.
<i>supports_getinfo</i>	Indicates whether the command supports dynamic probing for settings (first argument invoked == __GETINFO__ or __EXECUTE__).
<i>supports_rawargs</i>	Indicates whether the command supports raw arguments being passed to it or if it uses parsed arguments (where quotes are stripped).
<i>type</i>	Specifies the type of command.  The only valid value for this attribute is <code>python</code> .

## 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
<i>earliest_time</i>	String		For scheduled searches display all the scheduled times starting from this time (not just the next run time)
<i>latest_time</i>	String		For scheduled searches display all the scheduled times until this time (not just the next run time)
<i>listDefaultActionArgs</i>	Boolean		Indicates whether to list default actions.
<i>add_orphan_field</i>	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 <i>add_orphan_field</i> is set to <code>true</code> , the response includes the orphaned search indicators, either <code>0</code> to indicate that a search is not orphaned or <code>1</code> 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
<i>action.&lt;action_name&gt;</i>	Indicates whether the <code>&lt;action_name&gt;</code> is enabled or disabled for a particular search. For more information about the alert action options see the <code>alert_actions.conf</code> file.
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>	Overrides the setting defined for an action in the <code>alert_actions.conf</code> file with a new setting that is valid only for the search configuration to which it is applied.
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.auth_password</i>	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.
<i>action.email.auth_username</i>	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  <i>Note:</i> Your SMTP server might reject unauthenticated emails.
<i>action.email.bcc</i>	BCC email address to use if <code>action.email</code> is enabled.
<i>action.email.cc</i>	CC email address to use if <code>action.email</code> is enabled.
<i>action.email.command</i>	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 <code>\$</code> , for example to reference the savedsearch name use <code>\$name\$</code> , to reference the search use <code>\$search\$</code> .

Name	Description
<i>action.email.format</i>	Specify the format of text in the email. This value also applies to any attachments.  Valid values: (plain   html   raw   csv)
<i>action.email.from</i>	Email address from which the email action originates.
<i>action.email.hostname</i>	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. <i>Note:</i> 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.
<i>action.email.inline</i>	Indicates whether the search results are contained in the body of the email.  Results can be either inline or attached to an email. See <i>action.email.sendresults</i> .
<i>action.email.mailserver</i>	Set the address of the MTA server to be used to send the emails.  Defaults to <LOCALHOST> (or whatever is set in <i>alert_actions.conf</i> ).
<i>action.email.maxresults</i>	Sets the global maximum number of search results to send when email.action is enabled.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.preprocess_results</i>	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).  Usually the preprocessing consists of filtering out unwanted internal fields.
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.
<i>action.email.reportPaperSize</i>	Specifies the paper size for PDFs. Defaults to letter.  Valid values: (letter   legal   ledger   a2   a3   a4   a5)
<i>action.email.reportServerEnabled</i>	Not supported.
<i>action.email.reportServerURL</i>	Not supported.

Name	Description
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether to attach the search results in the email.  Results can be either attached or inline. See <i>action.email.inline</i> .
<i>action.email.subject</i>	Specifies an email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	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 <i>dispatch.ttl</i> in <i>savedsearches.conf</i> .  Valid values are Integer[p].
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server.
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server ( <i>starttls</i> ).
<i>action.populate_lookup</i>	The state of the populate lookup action.
<i>action.populate_lookup.command</i>	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\$.
<i>action.populate_lookup.hostname</i>	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 <i>action.email.hostname</i> for details.
<i>action.populate_lookup.maxresults</i>	The maximum number of search results sent using alerts.
<i>action.populate_lookup.maxtime</i>	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
<i>action.populate_lookup.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.populate_lookup.ttl</i>	<p>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.</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are Integer[p]</p>
<i>action.rss</i>	The state of the RSS action.
<i>action.rss.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.rss.hostname</i>	Sets the hostname used in the web link (url) sent in alert actions.
<i>action.rss.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.rss.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.
<i>action.rss.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.rss.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are: Integer[p]</p>
<i>action.script</i>	The state of the script action.
<i>action.script.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.script.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See <i>action.email.hostname</i> for details.</p>
<i>action.script.maxresults</i>	The maximum number of search results sent using alerts.

Name	Description
<i>action.script.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted.
<i>action.script.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.script.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by <i>dispatch.ttl</i> in <i>savedsearches.conf</i>.</p> <p>Valid values are: Integer[p]</p>
<i>action.summary_index</i>	Specifies whether the summary index action is enabled for this search.
<i>action.summary_index._type"</i>	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to <i>event</i> or <i>metric</i> .
<i>action.summary_index.force_realtime_schedule</i>	By default, <i>realtime_schedule</i> is <i>false</i> for a report configured for summary indexing. When set to <i>1</i> or <i>true</i> , this setting overrides <i>realtime_schedule</i> . Setting this setting to <i>true</i> can cause gaps in summary data, as a <i>realtime_schedule</i> search is skipped if search concurrency limits are violated.
<i>action.summary_index.inline</i>	<p>Determines whether to execute the summary indexing action as part of the scheduled search.</p> <p><b>Note:</b> This option is considered only if the summary index action is enabled and is always executed (in other words, if <i>counttype</i> = <i>always</i>).</p>
<i>action.summary_index.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.summary_index.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.
<i>action.summary_index.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.summary_index.ttl</i>	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.
<i>alert.digest_mode</i>	Indicates if alert actions are applied to the entire result set or to each individual result.
<i>alert.expires</i>	<p>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</p> <p>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p>
<i>alert.managedBy</i>	Specifies the feature or component that created the alert.
<i>alert.severity</i>	<p>The alert severity level.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>1 DEBUG</li> <li>2 INFO</li> <li>3 WARN</li> <li>4 ERROR</li> <li>5 SEVERE</li> <li>6 FATAL</li> </ul>
<i>alert.suppress</i>	Indicates whether alert suppression is enabled for this scheduled search.

Name	Description
<i>alert.suppress.fields</i>	List of fields to use when suppressing per-result alerts. Must be specified if the digest mode is disabled and suppression is enabled.
<i>alert.suppress.group_name</i>	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.
<i>alert.suppress.period</i>	Specifies the suppression period. Only valid if <i>alert.suppress</i> is enabled.  Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
<i>alert.track</i>	Specifies whether to track the actions triggered by this scheduled search.  <i>auto</i> - (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.  <i>true</i> - Force alert tracking for this search. Default.  <i>false</i> - Disable alert tracking for this search.
<i>alert_comparator</i>	One of the following strings:  greater than less than equal to rises by drops by rises by perc drops by perc  Used with <i>alert_threshold</i> to trigger alert actions.
<i>alert_condition</i>	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.  <i>Note:</i> If you specify an <i>alert_condition</i> , do not set <i>counttype</i> , <i>relation</i> , or <i>quantity</i> .
<i>alert_threshold</i>	Valid values are: Integer[%]  Specifies the value to compare (see <i>alert_comparator</i> ) before triggering the alert actions. If expressed as a percentage, indicates value to use when <i>alert_comparator</i> is set to <i>rises by perc</i> or <i>"drops by perc."</i>
<i>alert_type</i>	What to base the alert on, overridden by <i>alert_condition</i> if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
<i>allow_skew</i>	Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.  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.

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. **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.  
*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  $1 / \langle \text{integer} \rangle$ .  
*dispatch.spawn\_process* 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.  
*dispatch.As* 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).  
*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 = 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:dict>
  </content>
</entry>

```

```

    <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
<i>action.&lt;action_name&gt;</i>	Boolean	Enable or disable an alert action. See <code>alert_actions.conf</code> for available alert action types.  <i>action_name</i> defaults to an empty string.
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>		Use this syntax to configure action parameters. See <code>alert_actions.conf</code> for parameter options.
<i>action.summary_index._type"</i>	String	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to

Name	Type	Description
		event or metric.
<i>action.summary_index.force_realtime_schedule</i>	Boolean	By default, <i>realtime_schedule</i> is <i>false</i> for a report configured for summary indexing. When set to <i>1</i> or <i>True</i> , this setting overrides <i>realtime_schedule</i> . Setting this setting to <i>true</i> can cause gaps in summary data, as a <i>realtime_schedule</i> search is skipped if search concurrency limits are violated.
<i>actions</i>	String	A comma-separated list of actions to enable.  For example: rss,email
<i>alert.digest_mode</i>	Boolean	Specifies whether alert actions are applied to the entire result set or on each individual result. Defaults to <i>1</i> .
<i>alert.expires</i>	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.
<i>alert.severity</i>	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
<i>alert.suppress</i>	Boolean	Indicates whether alert suppression is enabled for this scheduled search.
<i>alert.suppress.fields</i>	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.
<i>alert.suppress.group_name</i>	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.
<i>alert.suppress.period</i>	Number	Valid values: [number][time-unit]  Specifies the suppression period. Only valid if <i>alert.suppress</i> is enabled.  Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
<i>alert.track</i>	String	Valid values: (true   false   auto)  Specifies whether to track the actions triggered by this scheduled search.

Name	Type	Description
		<p><code>auto</code> - 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.</p> <p><code>true</code> - Force alert tracking for this search.</p> <p><code>false</code> - Disable alert tracking for this search.</p>
<code>alert_comparator</code>	String	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc. Used with <code>alert_threshold</code> to trigger alert actions.
<code>alert_condition</code>	String	<p>Contains a conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</p> <p>Alerts are triggered if the specified search yields a non-empty search result list.</p> <p><b>Note:</b> If you specify an <code>alert_condition</code>, do not set <code>counttype</code>, <code>relation</code>, or <code>quantity</code>.</p>
<code>alert_threshold</code>	Number	<p>Valid values are: Integer[%]</p> <p>Specifies the value to compare (see <code>alert_comparator</code>) before triggering the alert actions. If expressed as a percentage, indicates value to use when <code>alert_comparator</code> is set to "rises by perc" or "drops by perc."</p>
<code>alert_type</code>	String	What to base the alert on, overridden by <code>alert_condition</code> if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
<code>allow_skew</code>	0   <percentage>   <duration>	<p>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods. Defaults to 0 (skew disabled).</p> <div> <p>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</p> </div>

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.

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.\*StringWildcard* 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.commandString* 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\_scheduleString* 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\_timeString* 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\_timeString* 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\_formatString* Defines the time format used to specify the earliest and latest time. Defaults to `%FT%T.%Q%:z`  
*auto\_summarize.dispatch.ttlString* 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*NumberThe maximum number of concurrent instances of this auto summarizing search that the scheduler is allowed to run.*auto\_summarize.max\_disabled\_buckets*NumberThe 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*NumberThe 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*NumberThe minimum summary size, in bytes, before testing whether the summarization is helpful.

The default value, 52428800, is equivalent to 5MB.

*auto\_summarize.max\_time*NumberThe 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*StringThe amount of time to suspend summarization of this search if the summarization is deemed unhelpful. Defaults to 24h.*auto\_summarize.timespan*StringComma-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*StringValid 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.

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*StringHuman-readable description of this saved search. Defaults to empty string.*disabled*BooleanIndicates whether the saved search is enabled. Defaults to 0. Disabled saved searches are not visible in Splunk Web.*dispatch.\**StringWildcard argument that accepts any dispatch related argument.*dispatch.allow\_partial\_results*BooleanSpecifies 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*NumberSpecifies the amount of inactive time, in seconds, after which the search job is automatically canceled.*dispatch.auto\_pause*NumberSpecifies the amount of inactive time, in seconds, after which the search job is automatically paused.*dispatch.buckets*NumberThe maximum number of timeline buckets. Defaults to 0.*dispatch.earliest\_time*StringA 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*StringA time string that specifies the earliest index time for this search. Can be a relative or absolute time.*dispatch.index\_latest*StringA time string that specifies the latest index time for this saved search. Can be a relative or absolute time.*dispatch.indexedRealtime*BooleanIndicates whether to use indexed-realtime mode when doing real-time searches.*dispatch.indexedRealtimeOffset*NumberAllows 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*NumberAllows 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*StringA 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*BooleanEnables or disables the lookups for this search. Defaults to 1.*dispatch.max\_count*NumberThe maximum number of results before finalizing the search. Defaults to 500000.*dispatch.max\_time*NumberIndicates 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  $1 / \langle \text{integer} \rangle$ . *dispatch.spawn\_process* Boolean 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.

*dispatch.as* 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`.

*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. *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:

```
* 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.searchStringRequired`. The search to save.  
*vsidString* 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
<i>action.&lt;action_name&gt;</i>	Indicates whether the <i>&lt;action_name&gt;</i> is enabled or disabled for a particular search. For more information about the alert action options see the <code>alert_actions.conf</code> file.
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>	Overrides the setting defined for an action in the <code>alert_actions.conf</code> file with a new setting that is valid only for the search configuration to which it is applied.
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.auth_password</i>	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.
<i>action.email.auth_username</i>	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  <i>Note:</i> Your SMTP server might reject unauthenticated emails.
<i>action.email.bcc</i>	BCC email address to use if <code>action.email</code> is enabled.
<i>action.email.cc</i>	CC email address to use if <code>action.email</code> is enabled.
<i>action.email.command</i>	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\$.
<i>action.email.format</i>	Specify the format of text in the email. This value also applies to any attachments.<  Valid values: (plain   html   raw   csv)
<i>action.email.from</i>	Email address from which the email action originates.  Defaults to <code>splunk@\$LOCALHOST</code> or whatever value is set in <code>alert_actions.conf</code> .
<i>action.email.hostname</i>	Sets the hostname used in the web link (url) sent in email actions.  This value accepts two forms:  hostname (for example, <code>splunkserver</code> , <code>splunkserver.example.com</code> )  protocol://hostname:port (for example, <code>http://splunkserver:8000</code> , <code>https://splunkserver.example.com:443</code> )

Name	Description
	<p>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.</p> <p>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.</p> <p>Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.</p>
<i>action.email.inline</i>	<p>Indicates whether the search results are contained in the body of the email.</p> <p>Results can be either inline or attached to an email. See <i>action.email.sendresults</i>.</p>
<i>action.email.mailserver</i>	<p>Set the address of the MTA server to be used to send the emails.</p> <p>Defaults to &lt;LOCALHOST&gt; (or whatever is set in <i>alert_actions.conf</i>).</p>
<i>action.email.maxresults</i>	Sets the global maximum number of search results to send when email.action is enabled.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.pdfview</i>	The name of the view to deliver if sendpdf is enabled
<i>action.email.preprocess_results</i>	<p>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).</p> <p>Usually the preprocessing consists of filtering out unwanted internal fields.</p>
<i>action.email.reportCIDFontList</i>	<p>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.</p> <p>If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used.</p> <p>To skip loading any CID fonts, specify the empty string.</p> <p>Default value: "gb cns jp kor"</p>
<i>action.email.reportIncludeSplunkLogo</i>	Indicates whether to include the Splunk logo with the report.
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.
<i>action.email.reportPaperSize</i>	<p>Specifies the paper size for PDFs. Defaults to letter.</p> <p>Valid values: (letter   legal   ledger   a2   a3   a4   a5)</p>
<i>action.email.reportServerEnabled</i>	Not supported.
<i>action.email.reportServerURL</i>	Not supported.
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether to attach the search results in the email.

Name	Description
	Results can be either attached or inline. See action.email.inline.
<i>action.email.subject</i>	Specifies an email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	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].
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server.
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
<i>action.email.width_sort_columns</i>	Indicates whether columns should be sorted from least wide to most wide, left to right.  Only valid if format=text.
<i>action.populate_lookup</i>	Indicates the state of the populate lookup action.
<i>action.populate_lookup.command</i>	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\$.
<i>action.populate_lookup.dest</i>	Lookup name or path of the lookup to populate.
<i>action.populate_lookup.hostname</i>	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.
<i>action.populate_lookup.maxresults</i>	The maximum number of search results sent using alerts.
<i>action.populate_lookup.maxtime</i>	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]
<i>action.populate_lookup.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.

Name	Description
<i>action.populate_lookup.ttl</i>	<p>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.</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are Integer[p]</p>
<i>action.rss</i>	Indicates the state of the RSS action.
<i>action.rss.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.rss.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See action.email.hostname for details.</p>
<i>action.rss.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.rss.maxtime</i>	<p>Sets the maximum amount of time the execution of an action takes before the action is aborted.</p> <p>Valid values are Integer[m  s  h  d].</p>
<i>action.rss.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.rss.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are: Integer[p]</p>
<i>action.script</i>	Indicates the state of the script for this action.
<i>action.script.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.script.filename</i>	File name of the script to call. Required if script action is enabled

Name	Description
<i>action.script.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See <code>action.email.hostname</code> for details.</p>
<i>action.script.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.script.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted.
<i>action.script.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.script.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by <code>dispatch.ttl</code> in <code>savedsearches.conf</code>.</p> <p>Valid values are: Integer[p]</p>
<i>action.summary_index</i>	Indicates the state of the summary index.
<i>action.summary_index._name</i>	<p>Specifies the name of the summary index where the results of the scheduled search are saved.</p> <p>Defaults to "summary."</p>
<i>action.summary_index.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.summary_index.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See <code>action.email.hostname</code> for details.</p>
<i>action.summary_index.inline</i>	<p>Determines whether to execute the summary indexing action as part of the scheduled search.</p> <p><i>Note:</i> This option is considered only if the summary index action is enabled and is always executed (in other words, if <code>counttype = always</code>).</p>
<i>action.summary_index.maxresults</i>	Sets the maximum number of search results sent using alerts.

Name	Description
<i>action.summary_index.maxtime</i>	<p>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</p> <p>Valid values are: Integer[m s h d]</p>
<i>action.summary_index.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.summary_index.ttl</i>	<p>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.</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are: Integer[p]</p>
<i>actions</i>	Actions triggered by this alert.
<i>alert.digest_mode</i>	Indicates if the alert actions are applied to the entire result set or to each individual result.
<i>alert.expires</i>	<p>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</p> <p>Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p> <p>Valid values: [number][time-unit]</p>
<i>alert.severity</i>	<p>Valid values: (1   2   3   4   5   6)</p> <p>Sets the alert severity level.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>1 DEBUG</li> <li>2 INFO</li> <li>3 WARN</li> <li>4 ERROR</li> <li>5 SEVERE</li> <li>6 FATAL</li> </ul>
<i>alert.suppress</i>	Indicates whether alert suppression is enabled for this scheduled search.
<i>alert.suppress.fields</i>	Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
<i>alert.suppress.period</i>	<p>Specifies the suppression period. Only valid if alert.suppress is enabled.</p> <p>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p>
<i>alert.track</i>	<p>Specifies whether to track the actions triggered by this scheduled search.</p> <p>auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.</p> <p>true - force alert tracking.</p>



Name	Description
	false - disable alert tracking for this search.
<i>alert_comparator</i>	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc
<i>alert_condition</i>	<p>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</p> <p>Alerts are triggered if the specified search yields a non-empty search result list.</p> <p><i>Note:</i> If you specify an alert_condition, do not set counttype, relation, or quantity.</p>
<i>alert_threshold</i>	<p>Valid values are: Integer[%]</p> <p>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."</p>
<i>alert_type</i>	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.
<i>allow_skew</i>	<p>0   &lt;percentage&gt;   &lt;duration&gt;</p> <p>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.</p> <div> <p>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</p> </div>

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

*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.

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 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.indexedRealtime* Indicates whether to use 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 backfill the real time window for this search. Parameter valid only if this is a real time search. *dispatch.spawn\_process* 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`. *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\_search\_peer\_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*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:list>
    </s:key>
  </s:dict>
</s:key>

```

```

<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
<i>earliest_time</i>	String		If the search is scheduled display scheduled times starting from this time
<i>latest_time</i>	String		If the search is scheduled display scheduled times ending at this time
<i>listDefaultActionArgs</i>	Boolean		Indicates whether to list default actions.
<i>add_orphan_field</i>	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 <i>add_orphan_field</i> is set to <code>true</code> , 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
<i>action.&lt;action_name&gt;</i>	Indicates whether the <i>&lt;action_name&gt;</i> is enabled or disabled for a particular search. For more information about the alert action options see the <code>alert_actions.conf</code> file.
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>	Overrides the setting defined for an action in the <code>alert_actions.conf</code> file with a new setting that is valid only for the search configuration to which it is applied.

Name	Description
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.auth_password</i>	<p>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.</p> <p>Defaults to empty string.</p>
<i>action.email.auth_username</i>	<p>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.</p> <p><b>Note:</b> Your SMTP server might reject unauthenticated emails.</p>
<i>action.email.bcc</i>	BCC email address to use if action.email is enabled.
<i>action.email.cc</i>	CC email address to use if action.email is enabled.
<i>action.email.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.email.format</i>	<p>Specify the format of text in the email. This value also applies to any attachments.</p> <p>Valid values: (plain   html   raw   csv)</p>
<i>action.email.from</i>	Email address from which the email action originates.
<i>action.email.hostname</i>	<p>Sets the hostname used in the web link (url) sent in email actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>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.</p> <p>When this value begins with 'http://', it is used verbatim. <b>Note:</b> 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.</p> <p>Defaults to current hostname provided by the operating system, or if that fails "localhost." When set to empty, default behavior is used.</p>
<i>action.email.inline</i>	<p>Indicates whether the search results are contained in the body of the email.</p> <p>Results can be either inline or attached to an email. See action.email.sendresults.</p>

Name	Description
<i>action.email.mailserver</i>	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).
<i>action.email.maxresults</i>	Sets the global maximum number of search results to send when email.action is enabled.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.preprocess_results</i>	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).  Usually the preprocessing consists of filtering out unwanted internal fields.
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.
<i>action.email.reportPaperSize</i>	Specifies the paper size for PDFs. Defaults to letter.  Valid values: (letter   legal   ledger   a2   a3   a4   a5)
<i>action.email.reportServerEnabled</i>	Not supported.
<i>action.email.reportServerURL</i>	Not supported.
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether to attach the search results in the email.  Results can be either attached or inline. See action.email.inline.
<i>action.email.subject</i>	Specifies an email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	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].
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server.
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
<i>action.populate_lookup</i>	The state of the populate lookup action.
<i>action.populate_lookup.command</i>	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.

Name	Description
	To reference saved search field values wrap them in \$, for example to reference the savedsearch name use \$name\$, to reference the search use \$search\$.
<i>action.populate_lookup.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See action.email.hostname for details.</p>
<i>action.populate_lookup.maxresults</i>	The maximum number of search results sent using alerts.
<i>action.populate_lookup.maxtime</i>	<p>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</p> <p>Valid values are: Integer[m s h d]</p>
<i>action.populate_lookup.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.populate_lookup.ttl</i>	<p>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.</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are Integer[p]</p>
<i>action.rss</i>	The state of the RSS action.
<i>action.rss.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.rss.hostname</i>	Sets the hostname used in the web link (url) sent in alert actions.
<i>action.rss.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.rss.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.
<i>action.rss.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.rss.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are: Integer[p]</p>

Name	Description
<i>action.script</i>	The state of the script action.
<i>action.script.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.script.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See <i>action.email.hostname</i> for details.</p>
<i>action.script.maxresults</i>	The maximum number of search results sent using alerts.
<i>action.script.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted.
<i>action.script.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.script.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are: Integer[p]</p>
<i>action.summary_index</i>	The state of the summary index action.
<i>action.summary_index._name</i>	<p>Specifies the name of the summary index where the results of the scheduled search are saved.</p> <p>Defaults to "summary."</p>
<i>action.summary_index._type"</i>	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to <code>event</code> or <code>metric</code> .
<i>action.summary_index.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.summary_index.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p>

Name	Description
	<p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See action.email.hostname for details.</p>
<i>action.summary_index.force_realtime_schedule</i>	By default, <i>realtime_schedule</i> is <i>false</i> for a report configured for summary indexing. When set to <i>1</i> or <i>true</i> , this setting overrides <i>realtime_schedule</i> . Setting this setting to <i>true</i> can cause gaps in summary data, as a <i>realtime_schedule</i> search is skipped if search concurrency limits are violated.
<i>action.summary_index.inline</i>	<p>Determines whether to execute the summary indexing action as part of the scheduled search.</p> <p><i>Note:</i> This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).</p>
<i>action.summary_index.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.summary_index.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.
<i>action.summary_index.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.summary_index.ttl</i>	<p>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If <i>p</i> follows Integer, specifies the number of scheduled periods. Defaults to 10p.</p> <p>If no actions are triggered, the artifacts have their ttl determined by <i>dispatch.ttl</i> in <i>savedsearches.conf</i>.</p> <p>Valid values are: Integer[<i>p</i>]</p>
<i>alert.digest_mode</i>	Specifies whether alert actions are applied to the entire result set or to each individual result.
<i>alert.expires</i>	Sets the period of time to show the alert in the dashboard. Defaults to 24h.
<i>alert.managedBy</i>	Specifies the feature or component that created the alert.
<i>alert.severity</i>	<p>Valid values: (1   2   3   4   5   6)</p> <p>Sets the alert severity level.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>1 DEBUG</li> <li>2 INFO</li> <li>3 WARN</li> <li>4 ERROR</li> <li>5 SEVERE</li> <li>6 FATAL</li> </ul>
<i>alert.suppress</i>	Indicates whether alert suppression is enabled for this schedules search.
<i>alert.suppress.fields</i>	List of fields to use when suppressing per-result alerts. Must be specified if the digest mode is disabled and suppression is enabled.
<i>alert.suppress.group_name</i>	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.

Name	Description
<i>alert.suppress.period</i>	<p>Specifies the suppression period. Only valid if alert.suppress is enabled.</p> <p>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p>
<i>alert.track</i>	<p>Specifies whether to track the actions triggered by this scheduled search.</p> <p><i>auto</i> - (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.</p> <p><i>true</i> - Force alert tracking for this search. Default.</p> <p><i>false</i> - Disable alert tracking for this search.</p>
<i>alert_comparator</i>	<p>One of the following strings:</p> <ul style="list-style-type: none"> <li>greater than</li> <li>less than</li> <li>equal to</li> <li>rises by</li> <li>drops by</li> <li>rises by perc</li> <li>drops by perc</li> </ul> <p>Used with <i>alert_threshold</i> to trigger alert actions.</p>
<i>alert_condition</i>	<p>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.</p> <p><i>Note:</i> If you specify an <i>alert_condition</i>, do not set counttype, relation, or quantity.</p>
<i>alert_threshold</i>	<p>Valid values are: Integer[%]</p> <p>Specifies the value to compare (see <i>alert_comparator</i>) before triggering the alert actions. If expressed as a percentage, indicates value to use when <i>alert_comparator</i> is set to <i>rises by perc</i> or <i>drops by perc</i>."</p>
<i>alert_type</i>	<p>What to base the alert on, overridden by <i>alert_condition</i> 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.</p>
<i>allow_skew</i>	<p>0   &lt;percentage&gt;   &lt;duration&gt;</p> <p>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.</p> <div> <p>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</p> </div>

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.

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. **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. *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  $1 / \langle \text{integer} \rangle$ . *dispatch.spawn\_process* Indicates whether a new search process spawns when this saved search is executed. *dispatch.time\_formatA* 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. *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)
```

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</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:list>
    </s:key>
  </s:dict>
</s:key>

```

```

<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
<i>action.&lt;action_name&gt;</i>	Boolean	Enable or disable an alert action. See <code>alert_actions.conf</code> for available alert action types.  <i>action_name</i> defaults to the empty string.
<i>action.&lt;action_name&gt;.&lt;parameter&gt;</i>	String or Number	Use this syntax to configure action parameters. See <code>alert_actions.conf</code> for parameter options.
<i>action.summary_index._type</i>	String	Specifies the data type of the summary index where the Splunk software saves the results of the scheduled search. Can be set to <code>event</code> or <code>metric</code> .
<i>action.summary_index.force_realtime_schedule</i>	Boolean	By default, <i>realtime_schedule</i> is <code>false</code> for a report configured for summary indexing. When set to <code>1</code> or <code>True</code> , this setting overrides <i>realtime_schedule</i> . Setting this setting to <code>true</code> can cause gaps in summary data, as a <i>realtime_schedule</i> search is skipped if search concurrency limits are violated.
<i>actions</i>	String	A comma-separated list of actions to enable.  For example: <code>rss,email</code>
<i>alert.digest_mode</i>	Boolean	Specifies whether alert actions are applied to the entire result set or on each individual result. Defaults to <code>1</code> ( <code>true</code> ).
<i>alert.expires</i>	Number	Valid values: <code>[number][time-unit]</code>  Sets the period of time to show the alert in the dashboard. Defaults to <code>24h</code> .  Use <code>[number][time-unit]</code> to specify a time. For example: <code>60</code> = 60 seconds, <code>1m</code> = 1 minute, <code>1h</code> = 60 minutes = 1 hour.
<i>alert.severity</i>	Enum	Valid values: <code>(1   2   3   4   5   6)</code>  Sets the alert severity level.  Valid values are:  <code>1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL</code>  Defaults to <code>3</code> .
<i>alert.suppress</i>	Boolean	Indicates whether alert suppression is enabled for this scheduled search.
<i>alert.suppress.fields</i>	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.
<i>alert.suppress.group_name</i>	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.
<i>alert.suppress.period</i>	Number	Valid values: <code>[number][time-unit]</code>

Name	Type	Description
		<p>Specifies the suppression period. Only valid if <i>alert.suppress</i> is enabled.</p> <p>Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p>
<i>alert.track</i>	Enum	<p>Valid values: (true   false   auto)</p> <p>Specifies whether to track the actions triggered by this scheduled search.</p> <p><i>auto</i> - 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.</p> <p><i>true</i> - Force alert tracking for this search.</p> <p><i>false</i> - Disable alert tracking for this search.</p>
<i>alert_comparator</i>	String	<p>One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc. Used with <i>alert_threshold</i> to trigger alert actions.</p>
<i>alert_condition</i>	String	<p>Contains a conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</p> <p>Alerts are triggered if the specified search yields a non-empty search result list.</p> <p><b>Note:</b> If you specify an <i>alert_condition</i>, do not set <i>counttype</i>, <i>relation</i>, or <i>quantity</i>.</p>
<i>alert_threshold</i>	Number	<p>Valid values are: Integer[%]</p> <p>Specifies the value to compare (see <i>alert_comparator</i>) before triggering the alert actions. If expressed as a percentage, indicates value to use when <i>alert_comparator</i> is set to "rises by perc" or "drops by perc."</p>
<i>alert_type</i>	String	<p>What to base the alert on, overridden by <i>alert_condition</i> if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.</p>
<i>allow_skew</i>	0   <percentage>   <duration>	<p>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.</p> <p>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</p>

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.

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.*StringWildcard` 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.commandString` 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_scheduleString` 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_timeString` 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*StringA 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*StringDefines the time format that Splunk software uses to specify the earliest and latest time. Defaults to %FT%T. %Q%:z *auto\_summarize.dispatch.ttl*StringValid 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*NumberThe 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*NumberThe 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*NumberThe 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*NumberMaximum 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*StringTime specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful. Defaults to 24h. *auto\_summarize.timespan*StringComma-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*StringValid 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.

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*StringHuman-readable description of this saved search. Defaults to empty string. *disabled*BooleanIndicates if the saved search is enabled. Defaults to 0.

Disabled saved searches are not visible in Splunk Web.

*dispatch.\**StringWildcard argument that accepts any dispatch related argument. *dispatch.allow\_partial\_results*BooleanSpecifies 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*NumberSpecifies the amount of inactive time, in seconds, after which the search job is automatically canceled. *dispatch.auto\_pause*NumberSpecifies the amount of inactive time, in seconds, after which the search job is automatically

paused.*dispatch.buckets*NumberThe maximum number of timeline buckets. Defaults to 0.*dispatch.earliest\_time*StringA 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*StringA time string that specifies the earliest index time for this search. Can be a relative or absolute time.*dispatch.index\_latest*StringA time string that specifies the latest index time for this saved search. Can be a relative or absolute time.*dispatch.indexedRealtime*BooleanIndicates whether to use indexed-realtime mode when doing real-time searches.*dispatch.indexedRealtimeOffset*IntegerAllows 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*IntegerAllows 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*StringA 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*BooleanEnables or disables the lookups for this search. Defaults to 1.*dispatch.max\_count*NumberThe maximum number of results before finalizing the search. Defaults to 500000.*dispatch.max\_time*NumberIndicates the maximum amount of time (in seconds) before finalizing the search. Defaults to 0.*dispatch.reduce\_freq*NumberSpecifies, in seconds, how frequently the MapReduce reduce phase runs on accumulated map values. Defaults to 10.*dispatch.rt\_backfill*BooleanWhether 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*NumberAllows 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*NumberThe integer value used to calculate the sample ratio. The formula is  $1 / \langle \text{integer} \rangle$ .*dispatch.spawn\_process*BooleanSpecifies 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*StringA time format string that defines the time format for specifying the earliest and latest time. Defaults to `%FT%T.%Q%:z`*dispatch.ttl*NumberValid 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*StringWhen 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*StringDefines 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*StringSpecifies 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.  *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.

Set to `auto` to let the scheduler determine the optimal window value automatically. Requires the `edit_search_schedule_window` capability to override `auto`.

**searchStringRequired.** 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`.

`vsidString` Defines the viewstate id associated with the UI view listed in 'displayview'. Must match up to a stanza in `viewstates.conf.workload_poolString` Specifies the new workload pool where the existing running search will be placed.

## Returned values

Name	Description
<code>action.&lt;action_name&gt;</code>	Indicates whether the <code>&lt;action_name&gt;</code> is enabled or disabled for a particular search. For more information about the alert action options see the <code>alert_actions.conf</code> file.
<code>action.&lt;action_name&gt;.&lt;parameter&gt;</code>	Overrides the setting defined for an action in the <code>alert_actions.conf</code> file with a new setting that is valid only for the search configuration to which it is applied.
<code>action.email</code>	Indicates the state of the email action.
<code>action.email.auth_password</code>	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.
<code>action.email.auth_username</code>	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  <i>Note:</i> Your SMTP server might reject unauthenticated emails.
<code>action.email.bcc</code>	BCC email address to use if action.email is enabled.
<code>action.email.cc</code>	CC email address to use if action.email is enabled.
<code>action.email.command</code>	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\$.
<code>action.email.format</code>	Specify the format of text in the email. This value also applies to any attachments.<  Valid values: (plain   html   raw   csv)
<code>action.email.from</code>	Email address from which the email action originates.

Name	Description
	Defaults to splunk@\$LOCALHOST or whatever value is set in alert_actions.conf.
<i>action.email.hostname</i>	<p>Sets the hostname used in the web link (url) sent in email actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>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.</p> <p>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.</p> <p>Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.</p>
<i>action.email.inline</i>	<p>Indicates whether the search results are contained in the body of the email.</p> <p>Results can be either inline or attached to an email. See action.email.sendresults.</p>
<i>action.email.mailserver</i>	<p>Set the address of the MTA server to be used to send the emails.</p> <p>Defaults to &lt;LOCALHOST&gt; (or whatever is set in alert_actions.conf).</p>
<i>action.email.maxresults</i>	Sets the global maximum number of search results to send when email.action is enabled.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.pdfview</i>	The name of the view to deliver if sendpdf is enabled
<i>action.email.preprocess_results</i>	<p>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).</p> <p>Usually the preprocessing consists of filtering out unwanted internal fields.</p>
<i>action.email.reportCIDFontList</i>	<p>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.</p> <p>If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used.</p> <p>To skip loading any CID fonts, specify the empty string.</p> <p>Default value: "gb cns jp kor"</p>
<i>action.email.reportIncludeSplunkLogo</i>	Indicates whether to include the Splunk logo with the report.
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.

Name	Description
<i>action.email.reportPaperSize</i>	Specifies the paper size for PDFs. Defaults to letter.  Valid values: (letter   legal   ledger   a2   a3   a4   a5)
<i>action.email.reportServerEnabled</i>	Not supported.
<i>action.email.reportServerURL</i>	Not supported.
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether to attach the search results in the email.  Results can be either attached or inline. See <i>action.email.inline</i> .
<i>action.email.subject</i>	Specifies an email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	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 <i>dispatch.ttl</i> in <i>savedsearches.conf</i> .  Valid values are Integer[p].
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server.
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server ( <i>starttls</i> ).
<i>action.email.width_sort_columns</i>	Indicates whether columns should be sorted from least wide to most wide, left to right.  Only valid if <i>format=text</i> .
<i>action.populate_lookup</i>	Indicates the state of the populate lookup action.
<i>action.populate_lookup.command</i>	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\$.
<i>action.populate_lookup.dest</i>	Lookup name or path of the lookup to populate.
<i>action.populate_lookup.hostname</i>	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)

Name	Description
	<p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See action.email.hostname for details.</p>
<i>action.populate_lookup.maxresults</i>	The maximum number of search results sent using alerts.
<i>action.populate_lookup.maxtime</i>	<p>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</p> <p>Valid values are: Integer[m s h d]</p>
<i>action.populate_lookup.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.populate_lookup.ttl</i>	<p>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.</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are Integer[p]</p>
<i>action.rss</i>	Indicates the state of the RSS action.
<i>action.rss.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.rss.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See action.email.hostname for details.</p>
<i>action.rss.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.rss.maxtime</i>	<p>Sets the maximum amount of time the execution of an action takes before the action is aborted.</p> <p>Valid values are Integer[m  s  h  d].</p>
<i>action.rss.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.rss.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p>



Name	Description
	Valid values are: Integer[p]
<i>action.script</i>	Indicates the state of the script for this action.
<i>action.script.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.script.filename</i>	File name of the script to call. Required if script action is enabled
<i>action.script.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See <i>action.email.hostname</i> for details.</p>
<i>action.script.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.script.maxtime</i>	Sets the maximum amount of time the execution of an action takes before the action is aborted.
<i>action.script.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.script.ttl</i>	<p>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).</p> <p>If no actions are triggered, the artifacts have their ttl determined by <i>dispatch.ttl</i> in <i>savedsearches.conf</i>.</p> <p>Valid values are: Integer[p]</p>
<i>action.summary_index</i>	Indicates the state of the summary index.
<i>action.summary_index._name</i>	<p>Specifies the name of the summary index where the results of the scheduled search are saved.</p> <p>Defaults to "summary."</p>
<i>action.summary_index.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.summary_index.hostname</i>	<p>Sets the hostname used in the web link (url) sent in alert actions.</p> <p>This value accepts two forms:</p> <p>hostname (for example, splunkserver, splunkserver.example.com)</p>

Name	Description
	<p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>See <code>action.email.hostname</code> for details.</p>
<code>action.summary_index.inline</code>	<p>Determines whether to execute the summary indexing action as part of the scheduled search.</p> <p><b>Note:</b> This option is considered only if the summary index action is enabled and is always executed (in other words, if <code>counttype = always</code>).</p>
<code>action.summary_index.maxresults</code>	Sets the maximum number of search results sent using alerts.
<code>action.summary_index.maxtime</code>	<p>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</p> <p>Valid values are: Integer[m s h d]</p>
<code>action.summary_index.track_alert</code>	Indicates whether the execution of this action signifies a trackable alert.
<code>action.summary_index.ttl</code>	<p>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.</p> <p>If no actions are triggered, the artifacts have their ttl determined by <code>dispatch.ttl</code> in <code>savedsearches.conf</code>.</p> <p>Valid values are: Integer[p]</p>
<code>actions</code>	Actions triggered by this alert.
<code>alert.digest_mode</code>	Indicates if the alert actions are applied to the entire result set or to each individual result.
<code>alert.expires</code>	<p>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</p> <p>Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p> <p>Valid values: [number][time-unit]</p>
<code>alert.severity</code>	<p>Valid values: (1   2   3   4   5   6)</p> <p>Sets the alert severity level.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>1 DEBUG</li> <li>2 INFO</li> <li>3 WARN</li> <li>4 ERROR</li> <li>5 SEVERE</li> <li>6 FATAL</li> </ul>
<code>alert.suppress</code>	Indicates whether alert suppression is enabled for this schedules search.
<code>alert.suppress.fields</code>	Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
<code>alert.suppress.period</code>	Specifies the suppression period. Only valid if <code>alert.supress</code> is enabled.

Name	Description
	Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.
<i>alert.track</i>	<p>Specifies whether to track the actions triggered by this scheduled search.</p> <p>auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.</p> <p>true - force alert tracking.</p> <p>false - disable alert tracking for this search.</p>
<i>alert_comparator</i>	One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc
<i>alert_condition</i>	<p>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</p> <p>Alerts are triggered if the specified search yields a non-empty search result list.</p> <p><i>Note:</i> If you specify an alert_condition, do not set counttype, relation, or quantity.</p>
<i>alert_threshold</i>	<p>Valid values are: Integer[%]</p> <p>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."</p>
<i>alert_type</i>	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.
<i>allow_skew</i>	<p>0   &lt;percentage&gt;   &lt;duration&gt;</p> <p>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.</p> <div style="border: 1px solid #ccc; background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</p> </div>

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

*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.

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 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.indexedRealtime*Indicates whether to use 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*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`.*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\_search\_peer\_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* 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:dict>
</content>

```

```

<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:list>
    </s:key>
  </s:dict>
</s:key>

```



```

<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		<p>The suppression key used in field-based suppression.</p> <p>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.</p>

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.*			<p>Arg values to create a saved search is the saved search is a template search.</p> <p>For example, specify arg.index_name to create the following search:</p> <p>search index=\$args.index_name\$   ...</p>

Name	Type	Default	Description
<i>dispatchAs</i>	String	"owner"   "user"	Indicate the user context, quota, and access rights for the saved search. The saved search runs according to the context indicated.
<i>dispatch.*</i>	String		Any <i>dispatch.*</i> field of the search that needs to be overridden when running the summary search.
<i>dispatch.adhoc_search_level</i>	String		Use one of the following search modes. [ <i>verbose</i>   <i>fast</i>   <i>smart</i> ]
<i>dispatch.now</i>	Boolean		Dispatch the search as if the specified time for this parameter was the current time.
<i>force_dispatch</i>	Boolean		Indicates whether to start a new search even if another instance of this search is already running.
<i>now</i>	String		[Deprecated] Use <i>dispatch.now</i> .
<i>replay_speed</i>	Number greater than 0		<p>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.</p> <p><i>earliest_time</i> and <i>latest_time</i> arguments must indicate a real-time time range to use replay options.</p> <p>Use <i>replay_speed</i> with <i>replay_et</i> and <i>replay_lt</i> relative times to indicate a speed and time range for the replay. For example,</p> <pre>replay_speed = 10 replay_et = -d@d replay_lt = -@d</pre> <p>specifies a replay at 10x speed, as if the "wall clock" time starts yesterday at midnight and ends when it reaches today at midnight.</p> <p>For more information about using relative time modifiers, see Search time modifiers in the <i>Search reference</i>.</p>
<i>replay_et</i>	Time modifier string		Relative "wall clock" start time for the replay.
<i>replay_lt</i>	Time modifier string.		Relative end time for the replay clock. The replay stops when clock time reaches this time.
<i>trigger_actions</i>	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
<i>savedsearch</i>	<p>String triplet consisting of <code>user:app:search_name</code>. 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.</p> <p>As an example, the following parameter triplet represents an <code>admin</code> user, the <code>search</code> app context, and a search named <code>Splunk errors last 24 hours</code>.</p> <p><code>savedsearch=admin:search:Splunk%20errors%20last%2024%20hours</code></p>

### Returned values

Name	Description
<i>durableTrackTime</i>	The durable cursor <b>timestamp</b> for the search job, expressed in UNIX Epoch time notation (elapsed time since 1/1/1970). If <code>durableTrackType=_indextime</code> , this timestamp is associated with the indexed timestamp of the events returned by the job. If <code>durableTrackType=_time</code> , this timestamp is associated with the event timestamp of the events returned by the job.
<i>durableTrackType</i>	Indicates that a scheduled search is durable and specifies how the search tracks events. A value of <code>_time</code> means the durable search tracks each event by its event <b>timestamp</b> , based on time information included in the event. A value of <code>_indextime</code> 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 <code>none</code> .
<i>earliest_time</i>	The earliest time a search job is configured to start.
<i>isDone</i>	Indicates if the search has completed.
<i>isFinalized</i>	Indicates if the search was finalized (stopped before completion).
<i>isRealTimeSearch</i>	Indicates if the search is a real time search.
<i>isSaved</i>	Indicates if the search is saved indefinitely.
<i>isScheduled</i>	Indicates if the search is a scheduled search.
<i>isZombie</i>	Indicates if the process running the search is dead, but with the search not finished.
<i>latest_time</i>	The latest time a search job is configured to start.
<i>listDefaultActionArgs</i>	List default values of actions.*, even though some of the actions may not be specified in the saved search.
<i>ttl</i>	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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

        <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:dict>
                    <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
<i>schedule_time</i>	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
<i>earliest_time</i> required	String		Absolute or relative earliest time
<i>latest_time</i> required	String		Absolute or relative latest time

### Returned values

Name	Description
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.auth_password</i>	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.
<i>action.email.auth_username</i>	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  <i>Note:</i> Your SMTP server might reject unauthenticated emails.
<i>action.email.pdfview</i>	The name of the view to deliver if sendpdf is enabled.
<i>action.email.subject</i>	Specifies an email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.summary_index</i>	The state of the summary index action.
<i>action.summary_index._name</i>	The state of the summary index action.
<i>actions</i>	Actions triggered by this alert.
<i>alert.digest_mode</i>	Indicates if alert actions are applied to the entire result set or to each individual result.

Name	Description
<i>alert.expires</i>	<p>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</p> <p>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p>
<i>alert.severity</i>	<p>Valid values: (1   2   3   4   5   6)</p> <p>Sets the alert severity level.</p> <p>Valid values are:</p> <p>1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL</p>
<i>alert.suppress</i>	Indicates whether alert suppression is enabled for this scheduled search.
<i>alert.suppress.fields</i>	Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.
<i>alert.suppress.period</i>	<p>Specifies the suppression period. Only valid if <code>alert.suppress</code> is enabled.</p> <p>Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</p>
<i>alert.track</i>	<p>Specifies whether to track the actions triggered by this scheduled search.</p> <p>auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.</p> <p>true - force alert tracking.</p> <p>false - disable alert tracking for this search.</p>
<i>alert_comparator</i>	<p>Valid values are: Integer[%]</p> <p>Specifies the value to compare (see <code>alert_comparator</code>) before triggering the alert actions. If expressed as a percentage, indicates value to use when <code>alert_comparator</code> is set to "rises by perc" or "drops by perc."</p>
<i>alert_condition</i>	<p>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</p> <p>Alerts are triggered if the specified search yields a non-empty search result list.</p> <p><i>Note:</i> If you specify an <code>alert_condition</code>, do not set <code>counttype</code>, <code>relation</code>, or <code>quantity</code>.</p>
<i>alert_threshold</i>	<p>Valid values are: Integer[%]</p> <p>Specifies the value to compare (see <code>alert_comparator</code>) before triggering the alert actions. If expressed as a percentage, indicates value to use when <code>alert_comparator</code> is set to "rises by perc" or "drops by perc."</p>
<i>alert_type</i>	What to base the alert on, overridden by <code>alert_condition</code> if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
<i>cron_schedule</i>	The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.

Name	Description
	<p>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.</p> <p>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.</p> <p>Valid values: cron string</p>
<i>description</i>	Description of the saved search.
<i>disabled</i>	Indicates if this saved search is disabled.
<i>dispatch.buckets</i>	The maximum number of timeline buckets.
<i>dispatch.earliest_time</i>	<p>A time string that specifies the earliest time for this search. Can be a relative or absolute time.</p> <p>If this value is an absolute time, use the <code>dispatch.time_format</code> to format the value.</p>
<i>dispatch.latest_time</i>	<p>A time string that specifies the latest time for this saved search. Can be a relative or absolute time.</p> <p>If this value is an absolute time, use the <code>dispatch.time_format</code> to format the value.</p>
<i>dispatch.lookups</i>	Indicates if lookups are enabled for this search.
<i>dispatch.max_count</i>	The maximum number of results before finalizing the search.
<i>dispatch.max_time</i>	Indicates the maximum amount of time (in seconds) before finalizing the search
<i>earliest_time</i>	For scheduled searches display all the scheduled times starting from this time.
<i>is_scheduled</i>	Indicates if this search is to be run on a schedule.
<i>is_visible</i>	Indicates if this saved search appears in the visible saved search list.
<i>latest_time</i>	<p>A time string that specifies the latest time for this saved search. Can be a relative or absolute time.</p> <p>If this value is an absolute time, use the <code>dispatch.time_format</code> to format the value.</p>
<i>listDefaultActionArgs</i>	List default values of actions. *, even though some of the actions may not be specified in the saved search.
<i>max_concurrent</i>	The maximum number of concurrent instances of this search the scheduler is allowed to run.
<i>next_scheduled_time</i>	The time when the scheduler runs this search again.
<i>qualifiedSearch</i>	The exact search command for this saved search.
<i>realtime_schedule</i>	<p>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.</p> <p>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.</p>

Name	Description
	<p>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.</p> <p>The scheduler tries to execute searches that have <code>realtime_schedule</code> set to 1 before it executes searches that have continuous scheduling (<code>realtime_schedule = 0</code>).</p>
<code>request.ui_dispatch_app</code>	A field used by Splunk Web to denote the app this search should be dispatched in.
<code>request.ui_dispatch_view</code>	A field used by Splunk Web to denote the app this search should be dispatched in.
<code>restart_on_searchpeer_add</code>	<p>Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search.</p> <p><b>Note:</b> The peer can be a newly added peer or a peer down and now available.</p>
<code>run_on_startup</code>	<p>Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time.</p> <p>Splunk recommends that you set <code>run_on_startup</code> to true for scheduled searches that populate lookup tables.</p>
<code>scheduled_times</code>	The times when the scheduler runs the search.
<code>search</code>	<p>Search expression to filter the response. The response matches field values against the search expression. For example:</p> <p><code>search=foo</code> matches any object that has "foo" as a substring in a field.</p> <p><code>search=field_name%3Dfield_value</code> restricts the match to a single field. URI-encoding is required in this example.</p>
<code>vsid</code>	<p>The viewstate id associated with the Splunk Web view listed in 'displayview'.</p> <p>Matches to a stanza in <code>viewstates.conf</code>.</p>

### 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
<i>expiration</i>	String		Indicates the time the suppression period expires.
<i>key</i>			

### Returned values

Name	Description
<i>earliest_time</i>	For scheduled searches display all the scheduled times starting from this time.
<i>expiration</i>	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.
<i>latest_time</i>	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.
<i>listDefaultActionArgs</i>	List default values of actions.*, even though some of the actions may not be specified in the saved search.
<i>suppressed</i>	Indicates if alert suppression is enabled for this search.
<i>suppressionKey</i>	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
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.pdfview</i>	Name of the view to send as a PDF.

Name	Description
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether the search results are included in the email. The results can be attached or inline.
<i>action.email.to</i>	List of recipient email addresses. Required if the email alert action is enabled.
<i>action.email.ttl</i>	<p>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are Integer[p].</p>
<i>cron_schedule</i>	<p>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</p> <p>For example: */5 * * * * causes the search to execute every 5 minutes.</p> <p>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.</p> <p>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 (*/*) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.</p>
<i>description</i>	Description of this scheduled view object.
<i>disabled</i>	Indicates if the scheduled view is disabled.
<i>is_scheduled</i>	Indicates if PDF delivery of this view is scheduled.
<i>next_scheduled_time</i>	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
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.auth_password</i>	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.
<i>action.email.auth_username</i>	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  <i>Note:</i> Your SMTP server might reject unauthenticated emails.
<i>action.email.bcc</i>	"BCC email address to use if action.email is enabled.
<i>action.email.cc</i>	CC email address to use if action.email is enabled.
<i>action.email.command</i>	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
<i>action.email.format</i>	Specify the format of text in the email. This value also applies to any attachments.<  Valid values: (plain   html   raw   csv)
<i>action.email.from</i>	Email address from which the email action originates.  Defaults to splunk@\$LOCALHOST or whatever value is set in alert_actions.conf.
<i>action.email.hostname</i>	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 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.
<i>action.email.inline</i>	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.
<i>action.email.mailserver</i>	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).
<i>action.email.maxresults</i>	Sets the global maximum number of search results to send when email.action is enabled.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.pdfview</i>	The name of the view to deliver if sendpdf is enabled.
<i>action.email.preprocess_results</i>	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).  Usually the preprocessing consists of filtering out unwanted internal fields.
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.
<i>action.email.reportPaperSize</i>	Specifies the paper size for PDFs. Defaults to letter.  Valid values: (letter   legal   ledger   a2   a3   a4   a5)
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether to attach the search results in the email.

Name	Description
	Results can be either attached or inline. See action.email.inline.
<i>action.email.subject</i>	Specifies the email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	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].
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
<i>cron_schedule</i>	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
<i>description</i>	Description of this saved search for this view.
<i>disabled</i>	Indicates if the saved search for this view is disabled.
<i>is_scheduled</i>	Indicates if this search is to be run on a schedule.
<i>next_scheduled_time</i>	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:dict>
  </content>
</entry>

```

```

<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
<i>action.email.to</i> required	String		Comma or semicolon separated list of email addresses to send the view to
<i>action.email*</i>	String		Wildcard argument that accepts any email action.
<i>cron_schedule</i> 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.

Name	Type	Default	Description
			<p>For example: */5 * * * * causes the search to execute every 5 minutes.</p> <p>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.</p> <p>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.</p>
<i>description</i>	String		User readable description of this scheduled view object
<i>disabled</i>	Boolean	0	Whether this object is enabled or disabled
<i>is_scheduled_required</i>	Boolean		Whether this pdf delivery should be scheduled
<i>next_scheduled_time</i>	String		The next time when the view is delivered. Ignored on edit, here only for backwards compatability.

#### Returned values

Name	Description
<i>action.email</i>	Indicates the status of the email action.
<i>action.email.auth_password</i>	<p>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.</p> <p>Defaults to empty string.</p>
<i>action.email.auth_username</i>	<p>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.</p> <p><b>Note:</b> Your SMTP server might reject unauthenticated emails.</p>
<i>action.email.bcc</i>	BCC email address to use if action.email is enabled.
<i>action.email.cc</i>	CC email address to use if action.email is enabled.
<i>action.email.command</i>	<p>The search command (or pipeline) which is responsible for executing the action.</p> <p>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\$.</p>
<i>action.email.format</i>	<p>Specify the format of text in the email. This value also applies to any attachments.&lt;</p> <p>Valid values: (plain   html   raw   csv)</p>
<i>action.email.from</i>	Email address from which the email action originates
<i>action.email.hostname</i>	<p>Sets the hostname used in the web link (url) sent in email actions.</p> <p>This value accepts two forms:</p>

Name	Description
	<p>hostname (for example, splunkserver, splunkserver.example.com)</p> <p>protocol://hostname:port (for example, http://splunkserver:8000, https://splunkserver.example.com:443)</p> <p>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.</p> <p>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 an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable.</p> <p>Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used.</p>
<i>action.email.inline</i>	<p>Indicates whether the search results are contained in the body of the email.</p> <p>Results can be either inline or attached to an email. See <i>action.email.sendresults</i>.</p>
<i>action.email.mailserver</i>	<p>Set the address of the MTA server to be used to send the emails.</p> <p>Defaults to &lt;LOCALHOST&gt; (or whatever is set in <i>alert_actions.conf</i>).</p>
<i>action.email.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.pdfview</i>	The name of the view to deliver if <i>sendpdf</i> is enabled.
<i>action.email.preprocess_results</i>	<p>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).</p> <p>Usually the preprocessing consists of filtering out unwanted internal fields.</p>
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.
<i>action.email.reportPaperSize</i>	<p>Specifies the paper size for PDFs. Defaults to letter.</p> <p>Valid values: (letter   legal   ledger   a2   a3   a4   a5)</p>
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	<p>Indicates whether to attach the search results in the email.</p> <p>Results can be either attached or inline. See <i>action.email.inline</i>.</p>
<i>action.email.subject</i>	<p>Specifies an email subject.</p> <p>Defaults to <i>SplunkAlert-&lt;savedsearchname&gt;</i>.</p>
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	



Name	Description
	<p>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours).</p> <p>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</p> <p>Valid values are Integer[p].</p>
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server.
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).
<i>cron_schedule</i>	<p>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</p> <p>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.</p> <p>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.</p> <p>Valid values: cron string</p>
<i>description</i>	Description of the saved search for this view.
<i>disabled</i>	Indicates if the saved search for this view is disabled.
<i>is_scheduled</i>	Indicates if this search is to be run on a schedule.
<i>next_scheduled_time</i>	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 -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:dict>
  </content>
</entry>

```

```

<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
<i>args.*</i>	String		Wildcard argument that accepts any saved search template argument, such as arg.username=foobar when the search is search \$username\$.
<i>dispatch.*</i>	String		Wildcard argument that accepts any dispatch related argument.
<i>dispatch.now</i>	Boolean		Dispatch the search as if the specified time for this parameter was the current time.
<i>force_dispatch</i>	Boolean		Indicates whether to start a new search even if another instance of this search is already running.
<i>now</i>	String		[Deprecated] Use <i>dispatch.now</i> .
<i>trigger_actions</i>	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_X1NjaGVkdWx1ZFZpZXdfX015Vmlldw_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/MyView/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_X1NjaGVkdWx1ZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a</title>
    <id>https://localhost:8089/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWx1ZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a</id>
    <updated>2011-07-27T16:25:15-04:00</updated>
    <link
      href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWx1ZFZpZXdfX015Vmlldw_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_X1NjaGVkdWx1ZFZpZXdfX015Vmlldw_at_1311798300
```

```

_842d7ca298ab521a" rel="list"/>
  <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZGFZpZXdfX015Vmllldw_at_1311798300
_842d7ca298ab521a/_reload" rel="_reload"/>
  <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZGFZpZXdfX015Vmllldw_at_1311798300
_842d7ca298ab521a" rel="edit"/>
  <link
href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZGFZpZXdfX015Vmllldw_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
<i>schedule_time</i>	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
<i>earliest_time</i>	String		Absolute or relative earliest time
<i>latest_time</i>	String		Absolute or relative latest time

### Returned values

Name	Description
<i>action.email</i>	Indicates the state of the email action.
<i>action.email.auth_password</i>	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.
<i>action.email.auth_username</i>	The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  <i>Note:</i> Your SMTP server might reject unauthenticated emails.
<i>action.email.bcc</i>	BCC email address to use if action.email is enabled.
<i>action.email.cc</i>	CC email address to use if action.email is enabled.
<i>action.email.command</i>	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\$.
<i>action.email.format</i>	Specify the format of text in the email. This value also applies to any attachments.<  Valid values: (plain   html   raw   csv)
<i>action.email.from</i>	Email address from which the email action originates.
<i>action.email.hostname</i>	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 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.
<i>action.email.inline</i>	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.
<i>action.email.mailserver</i>	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).
<i>action.email.maxresults</i>	Sets the maximum number of search results sent using alerts.
<i>action.email.maxtime</i>	Specifies the maximum amount of time the execution of an email action takes before the action is aborted.
<i>action.email.pdfview</i>	The name of the view to deliver if sendpdf is enabled.
<i>action.email.preprocess_results</i>	Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).  Usually the preprocessing consists of filtering out unwanted internal fields.
<i>action.email.reportPaperOrientation</i>	Specifies the paper orientation: portrait or landscape.
<i>action.email.reportPaperSize</i>	Specifies the paper size for PDFs. Defaults to letter.  Valid values: (letter   legal   ledger   a2   a3   a4   a5)
<i>action.email.reportServerEnabled</i>	Not supported.

Name	Description
<i>action.email.reportServerURL</i>	Not supported.
<i>action.email.sendpdf</i>	Indicates whether to create and send the results as a PDF.
<i>action.email.sendresults</i>	Indicates whether to attach the search results in the email.  Results can be either attached or inline. See <i>action.email.inline</i> .
<i>action.email.subject</i>	Specifies an email subject.  Defaults to SplunkAlert-<savedsearchname>.
<i>action.email.to</i>	List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.
<i>action.email.track_alert</i>	Indicates whether the execution of this action signifies a trackable alert.
<i>action.email.ttl</i>	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 <i>dispatch.ttl</i> in <i>savedsearches.conf</i> .  Valid values are Integer[p].
<i>action.email.use_ssl</i>	Indicates whether to use SSL when communicating with the SMTP server.
<i>action.email.use_tls</i>	Indicates whether to use TLS (transport layer security) when communicating with the SMTP server ( <i>starttls</i> ).
<i>action.email.width_sort_columns</i>	Indicates whether columns should be sorted from least wide to most wide, left to right.  Only valid if <i>format=text</i> .
<i>cron_schedule</i>	The cron schedule to execute this search. For example: <i>*/5 * * * *</i> 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: <i>00,20,40 * * * *</i> , which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of <i>03,23,43 * * * *</i> 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 ( <i>*/20</i> ) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.  Valid values: cron string
<i>description</i>	Description of the saved search for this view.
<i>disabled</i>	Indicates if the saved search for this view is disabled.  Disabled saved searches are not visible in Splunk Web.
<i>is_scheduled</i>	Indicates if this search is to be run on a schedule.
<i>next_scheduled_time</i>	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:dict>
    </content>
  </entry>
</feed>
```

```

<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
<i>max_searches_perc</i>	Number	The maximum number of searches the scheduler can run as a percentage of the maximum number of concurrent searches. Default: 50%.
<i>auto_summary_perc</i>	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.
<i>max_searches_per_cpu</i>	Number	The maximum number of concurrent historical searches allowed per cpu. Default: 1.
<i>base_max_searches</i>	Number	A baseline constant to add to the max number of searches (computed as multiplier of the CPUs.) Default is 6.
<i>max_rt_search_multiplier</i>	Number	

Name	Type	Description
		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 $\text{max\_rt\_searches} = \text{max\_rt\_search\_multiplier} \times \text{max\_hist\_searches}$

## 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="efdcca30d13" 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:dict>
    </content>
  </entry>
</feed>
```

```

        </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
<i>max_searches_perc</i>	Number	The maximum number of searches the scheduler can run as a percentage of the maximum number of concurrent searches. Default: 50.
<i>auto_summary_perc</i>	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="efdcca30d13" 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:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

```

<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
<i>max_searches_per_cpu</i>	Number	The maximum number of concurrent historical searches allowed per cpu. Default: 1.
<i>base_max_searches</i>	Number	A baseline constant to add to the max number of searches (computed as multiplier of the CPUs.) Default is 6.
<i>max_rt_search_multiplier</i>	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 <code>max_rt_searches = max_rt_search_multiplier x max_hist_searches</code>

### 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="efdcca30d13" 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:dict>
    </content>
  </entry>
</feed>
```

```

    </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
<i>cursorTime</i>	The earliest time from which no events are later scanned.  Can be used to indicate progress. See description for doneProgress.
<i>custom</i>	Custom job property. (See the search/jobs POST request for an example of how to create a custom property.)  <i>Note:</i> 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.
<i>delegate</i>	For saved searches, specifies jobs that were started by the user. Defaults to scheduler.
<i>diskUsage</i>	The total amount of disk space used, in bytes.
<i>dispatchState</i>	The state of the search. Can be any of QUEUED, PARSING, RUNNING, PAUSED, FINALIZING, FAILED, DONE.
<i>doneProgress</i>	A number between 0 and 1.0 that indicates the approximate progress of the search.  $doneProgress = (latestTime \hat{=} cursorTime) / (latestTime \hat{=} earliestTime)$
<i>dropCount</i>	For real-time searches only, the number of possible events that were dropped due to the rt_queue_size (default to 100000).
<i>earliestTime</i>	The earliest time a search job is configured to start.  Can be used to indicate progress. See description for doneProgress.



Name	Description
<i>eventAvailableCount</i>	The number of events that are available for export.
<i>eventCount</i>	The number of events returned by the search.
<i>eventFieldCount</i>	The number of fields found in the search results.
<i>eventsIsStreaming</i>	Indicates if the events of this search are being streamed.
<i>eventsIsTruncated</i>	Indicates if events of the search are not stored, making them unavailable from the events endpoint for the search.
<i>eventPreviewableCount</i>	Number of in-memory events that are not yet committed to disk. Returned if <code>timeline_events_preview</code> is enabled in <code>limits.conf</code> .
<i>eventSearch</i>	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.
<i>eventSorting</i>	Indicates if the events of this search are sorted, and in which order.  asc = ascending;  desc = descending;  none = not sorted
<i>isDone</i>	Indicates if the search has completed.
<i>isEventPreviewEnabled</i>	Indicates if the <code>timeline_events_preview</code> setting is enabled in <code>limits.conf</code> .
<i>isFailed</i>	Indicates if there was a fatal error executing the search. For example, invalid search string syntax.
<i>isFinalized</i>	Indicates if the search was finalized (stopped before completion).
<i>isPaused</i>	Indicates if the search is paused.
<i>isPreviewEnabled</i>	Indicates if previews are enabled.
<i>isRealTimeSearch</i>	Indicates if the search is a real time search.
<i>isRemoteTimeline</i>	Indicates if the remote timeline feature is enabled.
<i>isSaved</i>	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 <code>default_save_ttl</code> value in <code>limits.conf</code> to override the default value of 7 days.
<i>isSavedSearch</i>	Indicates if this is a saved search run using the scheduler.
<i>isZombie</i>	Indicates if the process running the search is dead, but with the search not finished.
<i>keywords</i>	All positive keywords used by this search. A positive keyword is a keyword that is not in a NOT clause.
<i>label</i>	Custom name created for this search.
<i>latestTime</i>	The latest time a search job is configured to start.  Can be used to indicate progress. See description for <code>doneProgress</code> .
<i>messages</i>	Errors and debug messages.
<i>numPreviews</i>	Number of previews generated so far for this search job.
<i>performance</i>	A representation of the execution costs.
<i>priority</i>	An integer between 0-10 that indicates the search priority.

Name	Description
	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 <code>priority=5</code> .  <i>Note:</i> In *nix systems, non-privileged users can only reduce the priority of a process.
<i>remoteSearch</i>	The search string that is sent to every search peer.
<i>reportSearch</i>	If reporting commands are used, the reporting search.
<i>request</i>	GET arguments that the search sends to splunkd.
<i>resultCount</i>	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.
<i>resultsStreaming</i>	Indicates if the final results of the search are available using streaming (for example, no transforming operations).
<i>resultPreviewCount</i>	The number of result rows in the latest preview results.
<i>runDuration</i>	Time in seconds that the search took to complete.
<i>scanCount</i>	The number of events that are scanned or read off disk.
<i>searchEarliestTime</i>	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).
<i>searchLatestTime</i>	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).
<i>searchProviders</i>	A list of all the search peers that were contacted.
<i>sid</i>	The search ID number.
<i>statusBuckets</i>	Maximum number of timeline buckets.
<i>ttr</i>	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
PAUSED
FINALIZING
FAILED
DONE

```

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_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4</id>
    <updated>2011-06-21T10:10:31.000-07:00</updated>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4"
rel="alternate"/>
    <published>2011-06-21T10:10:23.000-07:00</published>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/search.log" rel="log"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/events" rel="events"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/results" rel="results"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/results_preview" rel="results_preview"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/timeline" rel="timeline"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/summary" rel="summary"/>
    <link
href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_at_1308676200_22702c154383bbe4/control" rel="control"/>
  </entry>
</feed>
```

```

<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 keepcolororder=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_VG9wIGZpdmUgc291cmNldHlwZXNlZXM_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:dict>
    </s:key>
  </s:dict>
</content>

```

```

</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
<i>adhoc_search_level</i>	String		Use one of the following search modes. [ <code>verbose</code>   <code>fast</code>   <code>smart</code> ]
<i>allow_partial_results</i>	Boolean	true	Indicates whether the search job can proceed to provide partial results if a search peer fails. When <code>false</code> , the search job fails if a search peer providing results for the search job fails.
<i>auto_cancel</i>	Number	0	If specified, the job automatically cancels after this many seconds of inactivity. (0 means never auto-cancel)
<i>auto_finalize_ec</i>	Number	0	Auto-finalize the search after at least this many events are processed.  Specify 0 to indicate no limit.
<i>auto_pause</i>	Number	0	If specified, the search job pauses after this many seconds of inactivity. (0 means never auto-pause)  To restart a paused search job, specify <code>unpause</code> as an action to <a href="#">POST search/jobs/{search_id}/control</a> .  <code>auto_pause</code> only goes into effect once. Unpausing after <code>auto_pause</code> does not put <code>auto_pause</code> into effect again.
<i>custom</i>	String		Specify a custom parameter (see example).
<i>earliest_time</i>	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 information.



Name	Type	Default	Description
			<p>examples of specifying a time string.</p> <p>Compare to <code>index_earliest</code> parameter. Also see comment for the <code>search_mode</code> parameter.</p>
<code>enable_lookups</code>	Boolean	true	<p>Indicates whether lookups should be applied to events.</p> <p>Specifying true (the default) may slow searches significantly depending on the number of lookups.</p>
<code>exec_mode</code>	Enum	normal	<p>Valid values: (blocking   oneshot   normal)</p> <p>If set to normal, runs an asynchronous search.</p> <p>If set to blocking, returns the sid when the job is complete.</p> <p>If set to oneshot, returns results in the same call. In this case, you can specify the output format (for example, json output) using the <code>output_mode</code> parameter as described in <a href="#">search/jobs/export</a>. Default format for output is xml. Does not return the search ID.</p>
<code>force_bundle_replication</code>	Boolean	false	<p>Specifies whether this search should cause (and wait depending on the value of <code>sync_bundle_replication</code>) bundle synchronization with all search peers.</p>
<code>id</code>	String		<p>Optional string to specify the search ID (<code>&lt;sid&gt;</code>). If unspecified, a random ID is generated.</p>
<code>index_earliest</code>	String		<p>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the specified time bounds.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time string (to now) or a formatted time string. Compare to <code>earliest_time</code> parameter. Also see comment for the <code>search_mode</code> parameter.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p>
<code>index_latest</code>	String		<p>Specify a time string. Sets the latest (exclusive), respectively, time bounds for the search, based on the specified time bounds.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time string (to now) or a formatted time string.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p> <p>Compare to <code>latest_time</code> parameter. Also see comment for the <code>search_mode</code> parameter.</p>
<code>indexedRealtime</code>	Boolean		<p>Indicate whether or not to use indexed-realtime mode for real-time searches.</p>
<code>indexedRealtimeOffset</code>	Number		<p>Set disk sync delay for indexed real-time search (seconds).</p>
<code>latest_time</code>	String		<p>Specify a time string. Sets the latest (exclusive), respectively, time bounds for the search.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time string (to now) or a formatted time string.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p> <p>Compare to <code>index_latest</code> parameter. Also see comment for the <code>search_mode</code> parameter.</p>

Name	Type	Default	Description
<i>max_count</i>	Number	10000	<p>The number of events that can be accessible in any given status bucket.</p> <p>Also, in transforming mode, the maximum number of results to store. Specifically, <code>codeoffset+count max_count</code>.</p>
<i>max_time</i>	Number	0	The number of seconds to run this search before finalizing. Specify 0 to never finalize.
<i>namespace</i>	String		<p>The application namespace in which to restrict searches.</p> <p>The namespace corresponds to the identifier recognized in the <code>/services/apps/1</code> endpoint.</p>
<i>now</i>	String	current system time	<p>Specify a time string to set the absolute time used for any relative time specifier in the search. Default is current system time.</p> <p>You can specify a relative time modifier for this parameter. For example, specify <code>+2d</code> to specify the current time plus two days.</p> <p>If you specify a relative time modifier both in this parameter and in the search string, the search string modifier takes precedence.</p> <p>Refer to Time modifiers for search for details on specifying relative time modifiers.</p>
<i>reduce_freq</i>	Number	0	Determines how frequently to run the MapReduce reduce phase on accumulated map values.
<i>reload_macros</i>	Boolean	true	<p>Specifies whether to reload macro definitions from <code>macros.conf</code>.</p> <p>Default is true.</p>
<i>remote_server_list</i>	String	empty list	Comma-separated list of (possibly wildcarded) servers from which raw events should be pulled. The server list is to be used in subsearches.
<i>replay_speed</i>	Number greater than 0		<p>Indicate a real-time search replay speed factor. For example, 1 indicates normal speed. 0.5 indicates half normal speed, and 2 indicates twice as fast as normal.</p> <p><code>earliest_time</code> and <code>latest_time</code> arguments must indicate a real-time time range to use with replay options.</p> <p>Use <i>replay_speed</i> with <i>replay_et</i> and <i>replay_lt</i> relative times to indicate a speed and time range for the replay. For example,</p> <pre>replay_speed = 10 replay_et = -d@d replay_lt = -@d</pre> <p>specifies a replay at 10x speed, as if the "wall clock" time starts yesterday at midnight and ends when it reaches today at midnight.</p> <p>For more information about using relative time modifiers, see Search time modifiers in the <i>Search reference</i>.</p>
<i>replay_et</i>	Time modifier string		Relative "wall clock" start time for the replay.

Name	Type	Default	Description
<i>replay_lt</i>	Time modifier string.		Relative end time for the replay clock. The replay stops when clock time reaches this time.
<i>required_field_list</i>	String	empty list	[Deprecated] Use <i>rf</i> .  A comma-separated list of required fields that, even if not referenced or used directly by the search, is still included by the events and summary endpoints. Splunk Web uses this list to prepopulate panels in the Search view.
<i>reuse_max_seconds_ago</i>	Number		Specifies the number of seconds ago to check when an identical search is started and return the job ID instead of starting a new job.
<i>rf</i>	String		Adds a required field to the search. There can be multiple <i>rf</i> POST arguments to the search.  These fields, even if not referenced or used directly by the search, are still included by the events and summary endpoints. Splunk Web uses these fields to prepopulate panels in the Search view.  Consider using this form of passing the required fields to the search instead of the deprecated <i>required_field_list</i> . If both <i>rf</i> and <i>required_field_list</i> are provided, the union of the two lists is used.
<i>rt_blocking</i>	Boolean	false	For a real-time search, indicates if the indexer blocks if the queue for this search is full.
<i>rt_indexfilter</i>	Boolean	true	For a real-time search, indicates if the indexer prefilters events.
<i>rt_maxblocksecs</i>	Number	60	For a real-time search with <i>rt_blocking</i> set to true, the maximum time to block.  Specify 0 to indicate no limit.
<i>rt_queue_size</i>	Number	10000 events	For a real-time search, the queue size (in events) that the indexer should use for this search.
<i>search required</i>	String		The search language string to execute, taking results from the local and remote servers.  Examples:  <pre>"search *" "search *   outputcsv"</pre>
<i>search_listener</i>	String		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/forward
<i>search_mode</i>	Enum	normal	Valid values: (normal   realtime)  If set to <i>realtime</i> , search runs over live data. A real-time search may also be indicated by the <i>earliest_time</i> and <i>latest_time</i> variables starting with 'rt' even if the <i>search_mode</i> is normal or is unset. For a real-time search, if both <i>earliest_time</i> and <i>latest_time</i> are

Name	Type	Default	Description
			<p>exactly 'rt', the search represents all appropriate live data received since the start of the search.</p> <p>Additionally, if <code>earliest_time</code> and/or <code>latest_time</code> are 'rt' followed by a relative time specifier, then a sliding window is used where the time bounds of the window are determined by the relative time specifiers and are continuously updated based on the wall-clock time.</p>
<code>spawn_process</code>	Boolean	true	<p>Specifies whether the search should run in a separate spawned process. Default is true.</p> <p>Searches against indexes <i>must</i> run in a separate process.</p>
<code>status_buckets</code>	Number	0	<p>The most status buckets to generate.</p> <p>0 indicates to not generate timeline information.</p>
<code>sync_bundle_replication</code>	Boolean		Specifies whether this search should wait for bundle replication to complete.
<code>time_format</code>	String	%FT%T.%Q%:z	Used to convert a formatted time string from {start,end}_time into UTC seconds. The default value is ISO-8601 format.
<code>timeout</code>	Number	86400	The number of seconds to keep this search after processing has stopped.
<code>workload_pool</code>	String		Specifies the new workload pool where the existing running search should be placed.

## Returned values

Name	Description
<code>sid</code>	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/jobs/export

`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`.

## 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
<i>auto_cancel</i>	Number		See the POST parameter descriptions for <code>search/jobs</code>
<i>auto_finalize_ec</i>	Number		See the POST parameter descriptions for <code>search/jobs</code>
<i>auto_pause</i>	Number		See the POST parameter descriptions for <code>search/jobs</code>

Name	Type	Default	Description
<i>earliest_time</i>	String		See the POST parameter descriptions for search/jobs
<i>enable_lookups</i>	Bool		See the POST parameter descriptions for search/jobs
<i>force_bundle_replication</i>	Bool		See the POST parameter descriptions for search/jobs
<i>id</i>	String		See the POST parameter descriptions for search/jobs
<i>index_earliest</i>	String		<p>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p>
<i>index_latest</i>	String		<p>Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p>
<i>latest_time</i>	String		See the POST parameter descriptions for search/jobs
<i>max_time</i>	Number		See the POST parameter descriptions for search/jobs
<i>namespace</i>	String		See the POST parameter descriptions for search/jobs
<i>now</i>	String		See the POST parameter descriptions for search/jobs
<i>output_mode</i>	Enum	xml	<p>Valid values: (atom   csv   json   json_cols   json_rows   raw   xml)</p> <p>Specifies the format for the returned output.</p>
<i>reduce_freq</i>	Number		See the POST parameter descriptions for search/jobs
<i>reload_macros</i>	Bool		See the POST parameter descriptions for search/jobs
<i>remote_server_list</i>	String		See the POST parameter descriptions for search/jobs
<i>required_field_list</i>	String		See the POST parameter descriptions for search/jobs
<i>rf</i>	String		See the POST parameter descriptions for search/jobs
<i>rt_blocking</i>	Bool		See the POST parameter descriptions for search/jobs
<i>rt_indexfilter</i>	Bool		See the POST parameter descriptions for search/jobs
<i>rt_maxblocksecs</i>	Number		See the POST parameter descriptions for search/jobs
<i>rt_queue_size</i>	Number		See the POST parameter descriptions for search/jobs
<i>search required</i>	String		See the POST parameter descriptions for search/jobs
<i>search_listener</i>	String		See the POST parameter descriptions for search/jobs
<i>search_mode</i>	Enum		See the POST parameter descriptions for search/jobs

Name	Type	Default	Description
<i>sync_bundle_replication</i>	Bool		See the POST parameter descriptions for search/jobs
<i>time_format</i>	String		See the POST parameter descriptions for search/jobs
<i>timeout</i>	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
<i>search</i>	String		See the parameters and returned values for search/jobs.
<i>auto_cancel</i>	Number		See the parameters and returned values for search/jobs.
<i>auto_finalize_ec</i>	Number		See the parameters and returned values for search/jobs.
<i>auto_pause</i>	Number		See the parameters and returned values for search/jobs.
<i>earliest_time</i>	String		See the parameters and returned values for search/jobs.
<i>enable_lookups</i>	Bool		See the parameters and returned values for search/jobs.



Name	Type	Default	Description
<i>force_bundle_replication</i>	Bool		See the parameters and returned values for search/jobs.
<i>id</i>	String		See the parameters and returned values for search/jobs.
<i>index_earliest</i>	String		<p>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p>
<i>index_latest</i>	String		<p>Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time.</p> <p>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</p> <p>Refer to Time modifiers for search for information and examples of specifying a time string.</p>
<i>latest_time</i>	String		See the parameters and returned values for search/jobs.
<i>max_time</i>	Number		See the parameters and returned values for search/jobs.
<i>namespace</i>	String		See the parameters and returned values for search/jobs.
<i>now</i>	String		See the parameters and returned values for search/jobs.
<i>output_mode</i>	Enum	xml	<p>Valid values: (atom   csv   json   json_cols   json_rows   raw   xml)</p> <p>Specifies the format for the returned output.</p>
<i>reduce_freq</i>	Number		See the parameters and returned values for search/jobs.
<i>reload_macros</i>	Bool		See the parameters and returned values for search/jobs.
<i>remote_server_list</i>	String		See the parameters and returned values for search/jobs.
<i>required_field_list</i>	String		See the parameters and returned values for search/jobs.
<i>rf</i>	String		See the parameters and returned values for search/jobs.
<i>rt_blocking</i>	Bool		See the parameters and returned values for search/jobs.
<i>rt_indexfilter</i>	Bool		See the parameters and returned values for search/jobs.
<i>rt_maxblocksecs</i>	Number		See the parameters and returned values for search/jobs.
<i>rt_queue_size</i>	Number		See the parameters and returned values for search/jobs.
<i>search_listener</i>	String		See the parameters and returned values for search/jobs.
<i>search_mode</i>	Enum		See the parameters and returned values for search/jobs.
<i>sync_bundle_replication</i>	Bool		See the parameters and returned values for search/jobs.
<i>time_format</i>	String		See the parameters and returned values for search/jobs.
<i>timeout</i>	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
PAUSED
FINALIZING
FAILED
DONE
```

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
------	------	---------	-------------

<i>action required</i>	Enum		<p>Valid values: (pause   unpause   finalize   cancel   touch   setttl   setpriority   enablepreview   disablepreview   setworkloadpool)</p> <p>The control action to execute.</p> <p>pause: Suspends the execution of the current search.</p> <p>unpause: Resumes the execution of the current search, if paused.</p> <p>finalize: Stops the search, and provides intermediate results to the /results endpoint.</p> <p>cancel: Stops the current search and deletes the result cache.</p> <p>touch: Extends the expiration time of the search to now + ttl</p> <p>setttl: Change the ttl of the search. Arguments: ttl=&lt;number&gt;</p> <p>setpriority: Sets the priority of the search process. Arguments: priority=&lt;0-10&gt;</p> <p>enablepreview: Enable preview generation (may slow search considerably).</p> <p>disablepreview: Disable preview generation.</p> <p>setworkloadpool: Moves a running search to a new workload pool. Arguments: workload_pool=&lt;string&gt;. Specifies the new workload pool. Requires edit_workload_pools capability.</p> <p>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.</p> <p>unsave: Disables any action performed by save.</p>

**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/jobs/{search\_id}/events**

https://<host>:<mPort>/services/search/jobs/{search\_id}/events

**Get {search\_id}** search events.



## GET

Access {search\_id} search events.

### Request parameters

Name	Type	Default	Description
<i>count</i>	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.
<i>earliest_time</i>	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.
<i>f</i>	String		A field to return for the event set.  You can pass multiple <code>POST f</code> arguments if multiple field are required. If <code>field_list</code> and <code>f</code> are provided, the union of the lists is used.
<i>field_list</i>	String	*	[Deprecated] Use <i>f</i> .  A comma-separated list of the fields to return for the event set.
<i>latest_time</i>	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.
<i>max_lines</i>	Number	0	The maximum lines that any single event <code>_raw</code> field should contain.  Specify 0 to specify no limit.
<i>offset</i>	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 <code>count</code> to compute the absolute offset (for example, <code>offset=-1</code> is the last available offset. Offsets in the results are always absolute and never negative.
<i>output_mode</i>	Enum	xml	Valid values: (atom   csv   json   json_cols   json_rows   raw   xml)  Specifies the format for the returned output.
<i>output_time_format</i>	String	<code>time_format</code>	Formats a UTC time. Defaults to what is specified in <code>time_format</code> .
<i>search</i>	String		The post processing search to apply to results. Can be any valid search language string.
<i>segmentation</i>	String	raw	The type of segmentation to perform on the data. This includes an option to perform k/v segmentation.
<i>time_format</i>	String	<code>%m/%d/%Y:%H:%M:%S</code>	Expression to convert a formatted time string from {start,end}_time into UTC seconds.
<i>truncation_mode</i>	Enum	abstract	Valid values: (abstract   truncate)  Specifies how "max_lines" should be achieved.

Name	Type	Default	Description

### 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/jobs/{search\_id}/results

https://<host>:<mPort>/services/search/jobs/{search\_id}/results

Get {search\_id} search results.

### GET

Get {search\_id} search results.

### Request parameters

Name	Type	Default	Description
<i>add_summary_to_metadata</i>	Boolean	false	Set the value to "true" to include field summary statistics in the response.
<i>count</i>	Number	100	The maximum number of results to return. If value is set to 0, then all available results are returned.
<i>f</i>	String		A field to return for the event set.  You can pass multiple <code>POST f</code> arguments if multiple field are required. If <code>field_list</code> and <code>f</code> are provided the union of the lists is used.
<i>field_list</i>	String		[Deprecated] Use <i>f</i> .  Specify a comma-separated list of the fields to return for the event set.
<i>offset</i>	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 <code>count</code> to compute the absolute offset (for example, <code>offset=-1</code> is the last available offset).  Offsets in the results are always absolute and never negative.
<i>output_mode</i>	Enum	xml	Valid values: (atom   csv   json   json_cols   json_rows   raw   xml)  Specifies the format for the returned output.

Name	Type	Default	Description
<i>search</i>	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 lisp: [ 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

`https://<host>:<mPort>/services/search/jobs/{search_id}/results_preview`

Preview {search\_id} search results.

## GET

Preview {search\_id} search results.

### Request parameters

Name	Type	Default	Description
<i>add_summary_to_metadata</i>	Boolean	false	Set the value to "true" to include field summary statistics in the response.
<i>count</i>	Number	100	The maximum number of results to return. If value is set to 0, then all available results are returned.
<i>f</i>	String		A field to return for the event set. You can pass multiple <code>POST f</code> arguments if multiple field are required. If <code>field_list</code> and <code>f</code> are provided the union of the lists is used.
<i>field_list</i>	String		[Deprecated] Use <i>f</i> . A comma-separated list of the fields to return for the event set.
<i>offset</i>	Number	0	The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0.
<i>output_mode</i>	Enum	xml	Valid values: (atom   csv   json   json_cols   json_rows   raw   xml) Specifies the format for the returned output.
<i>search</i>	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 lisp: [ 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>:<Port>/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
<i>attachment</i>	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](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
<i>earliest_time</i>	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 <code>search_mode</code> variable.)
<i>f</i>	String		A field to return for the event set.  You can pass multiple <code>POST f</code> arguments if multiple field are required. If <code>field_list</code> and <code>f</code> are provided, the union of the lists is used.
<i>field_list</i>	String		[Deprecated] Use <i>f</i> .  A comma-separated list of the fields to return for the event set.
<i>histogram</i>	Boolean	false	Indicates whether to add histogram data to the summary output.
<i>latest_time</i>	String		Time string representing the latest (exclusive), respectively, time bounds for the search.
<i>min_freq</i>	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.
<i>output_time_format</i>	String	<code>time_format</code>	Formats a UTC time.
<i>search</i>	String	Empty string	Specifies a substring that all returned events should contain either in one of their values or tags.
<i>time_format</i>	String	<code>%m/%d/%Y:%H:%M:%S</code>	Expression to convert a formatted time string from {start,end}_time into UTC seconds.
<i>top_count</i>	Number	10	For each key, specifies how many of the most frequent items to return.

Name	Type	Default	Description

## 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
<i>output_time_format</i>	String	<i>time_format</i>	Formats a UTC time.
<i>time_format</i>	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
<i>c</i>	Event count
<i>a</i>	Available. Not all events in a bucket are retrievable. Generally capped at 10000.
<i>t</i>	Time in epoch seconds
<i>d</i>	Bucket size (time)
<i>f</i>	Indicates if the search finished scanning events from the time range of this bucket.
<i>etz</i>	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.
<i>ltz</i>	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/parser

<https://<host>:<mPort>/services/search/parser>  
Get search language parsing.

### GET

Parses Splunk search language and returns semantic map.

### Request parameters

Name	Type	Default	Description
<i>enable_lookups</i>	Boolean	false	If <code>true</code> , reverse lookups are done to expand the search expression.
<i>output_mode</i>	String	xml	Specify output formatting. Select from either:  xml: XML formatting json: JSON formatting

Name	Type	Default	Description
<i>parse_only</i>	Boolean	false	If true, disables expansion of search due evaluation of subsearches, time term expansion, lookups, tags, eventtypes, sourcetype alias.
<i>q</i> required	String		The search string to parse.
<i>reload_macros</i>	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 keepcolororder=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
<i>saved_searches_disabled</i>	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
<i>disabled</i>	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
<i>now</i>	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 <code>time_format</code> .
<i>output_time_format</i>	String	%FT%T.%Q%:z	Used to format a UTC time. Defaults to the value of <code>time_format</code> .
<i>time required</i>	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.
<i>time_format</i>	String	%FT%T.%Q%:z	The format ( <code>strftime</code> ) 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
<i>count</i> required	Number		The number of items to return for this term.
<i>output_mode</i>	String	csv	Specify output formatting. Select from:  csv: CSV formatting xml: XML formatting json: JSON formatting
<i>prefix</i> 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
```

#### 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
}
]
```

} ]



# 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 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.

## 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
<i>help</i>	For internal use only
<i>&lt;message_name&gt;</i>	The message name depends on the specific message returned. This field might contain the same text as the <i>message</i> field.  In the following example response, this field is "manifest_error".
<i>message</i>	Message text
<i>server</i>	Name of the server that generated the error
<i>severity</i>	One of the following message severity values <ul style="list-style-type: none"><li>• info</li><li>• warn</li><li>• error</li></ul>
<i>timeCreated_epochSecs</i>	Timestamp when the message was posted
<i>timeCreated_iso</i>	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	<b>Required.</b> Message name (key).
capability	Comma separated list	One or more capabilities that users must have to view the message. Capability names are validated.
role	Comma separated list	One or more roles that users must have to view the message. Role names are validated.

Name	Type	Description
<i>value</i>	String	<b>Required.</b> Message text.
<i>severity</i>	String	One of the following message severity values. <ul style="list-style-type: none"> <li>• info</li> <li>• warn</li> <li>• error</li> </ul>

## 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
------	-------------

<i>help</i>	For internal use only
<i>&lt;message_name&gt;</i>	The message name depends on the specific message returned. This field might contain the same text as the <i>message</i> field.  In the following example response, this field is "manifest_error".
<i>message</i>	Message text
<i>server</i>	Name of the server that generated the error
<i>severity</i>	One of the following message severity values <ul style="list-style-type: none"> <li>• info</li> <li>• warn</li> <li>• error</li> </ul>
<i>timeCreated_epochSecs</i>	Timestamp when the message was posted
<i>timeCreated_iso</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:messages>
```

```

    <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
<i>name</i>	String	<b>Required.</b> 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
<i>http_proxy</i>	String	Identifies the server proxy. When set, splunkd sends all HTTP requests through the proxy server defined in <code>http_proxy</code> on the proxy. The default value is unset.
<i>https_proxy</i>	String	Identifies the server proxy. When set, splunkd sends all HTTPS requests through the proxy server defined in <code>https_proxy</code> . If not set, splunkd uses the <code>http_proxy</code> variable instead. The default value is unset.
<i>no_proxy</i>	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 <code>localhost/loopback</code> address are not proxied. The default value is <code>localhost, 127.0.0.1, ::1</code> .

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

```

<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
<i>http_proxy</i>	String	Identifies the server proxy. When set, splunkd sends all HTTP requests through the proxy server defined in <i>http_proxy</i> on the proxy. The default value is unset.
<i>https_proxy</i>	String	Identifies the server proxy. When set, splunkd sends all HTTPS requests through the proxy server defined in <i>https_proxy</i> . If not set, splunkd uses the <i>http_proxy</i> variable instead. The default value is unset.
<i>no_proxy</i>	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 <i>localhost/loopback</i> address are not proxied. The default value is <i>localhost, 127.0.0.1, ::1</i> .

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

```
</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
<i>level</i>	One of the following valid logger levels for this server. <ul style="list-style-type: none"><li>• FATAL</li><li>• WARN</li><li>• INFO</li><li>• DEBUG</li></ul>

### 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
<i>level</i>	<p>One of the following valid logger levels for this server.</p> <ul style="list-style-type: none"> <li>• FATAL</li> <li>• WARN</li> <li>• INFO</li> <li>• DEBUG</li> </ul>

## 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>
</s:messages>
</s:dict>
```

```
</content>
</entry>
```

POST

Set the logging level for a specific logging category.

Request parameters

Name	Type	Description
<i>level</i>	Enum	<b>Required.</b> 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
<variable>	<div>Zero or more of the following possible server roles.</div> <div><ul style="list-style-type: none"><li>• indexer</li><li>• universal_forwarder</li><li>• heavyweight_forwarder</li><li>• lightweight_forwarder</li><li>• license_master</li><li>• license_slave</li><li>• cluster_master</li><li>• cluster_slave</li><li>• cluster_search_head</li><li>• deployment_server</li><li>• deployment_client</li><li>• search_head</li><li>• search_peer</li><li>• shc_captain</li><li>• shc_deployer</li><li>• shc_member</li></ul></div>

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
<i>SPLUNK_DB</i>	Absolute filepath to the default index for this deployment.
<i>SPLUNK_HOME</i>	Absolute filepath to the local installation of this deployment.
<i>enableSplunkWebSSL</i>	Indicates if HTTPS and SSL are enabled for Splunk Web.
<i>host</i>	The default hostname to use for data inputs that do not override this setting.
<i>httpport</i>	Port on which Splunk Web listens for this instance. Defaults to 8000. If using SSL, set to the HTTPS port number.
<i>mgmtHostPort</i>	The port on which Splunk Web listens for management operations. Defaults to 8089.
<i>minFreeSpace</i>	<p>Safe amount of space in MB that must exist for splunkd to continue operating. <i>minFreespace</i> affects search and indexing in the following ways.</p> <ul style="list-style-type: none"><li>• Before attempting to launch a search, the Splunk platform requires this amount of free space on the filesystem where the dispatch directory is stored, <code>\$SPLUNK_HOME/var/run/splunk/dispatch</code>.</li><li>• Applied similarly to the search quota values in <code>authorize.conf</code> and <code>limits.conf</code>.</li><li>• For indexing, periodically, the indexer checks space on all partitions that contain splunk indexes as specified by <code>indexes.conf</code>. When you need to clear more disk space, indexing is paused and the Splunk platform posts a UI banner + warning.</li></ul>
<i>pass4SymmKey</i>	Password string prefixed to the Splunk platform symmetric key, generating the final key to sign all traffic between master/slave licenser.
<i>serverName</i>	Name identifying this instance for features such as distributed search.
<i>sessionTimeout</i>	<p>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.</p> <p>24h (24 hours)</p> <p>3d (3 days)</p> <p>7200s (7200 seconds, or two hours)</p>
<i>startwebserver</i>	Indicates whether Splunk Web is configured to start by default.
<i>trustedIP</i>	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 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, index cluster management endpoints are not applicable to Splunk Cloud deployments.

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

---

## 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
<i>cpu_weight</i>	Number	Specifies the fraction of the cpu assigned to this category as a ratio of the total of <code>cpu_weight</code> across all categories. This fraction is then applied to the cpu shares assigned to the parent group. The value must be > 0 and <= 100.
<i>mem_weight</i>	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="8c85clfbcc8c" 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
<i>cpu_weight</i>	Number	Specifies the fraction of the cpu assigned to this category as a ratio of the total of <i>cpu_weight</i> across all categories. This fraction is then applied to the cpu shares assigned to the parent group. The value must be > 0 and <= 100
<i>mem_weight</i>	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"/>
  </entry>
</feed>
```

```

<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
<i>cpu_weight</i>	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.
<i>mem_weight</i>	Number	Specifies the percentage of the memory assigned to this pool as a percent of the category. The total amount of memory limit for this pool is a percentage of the value assigned to the category.
<i>category</i>	string	Specifies the category in which a pool is created. Can be either "search", "ingest", or "misc".
<i>default_category_pool</i>	Boolean	Specifies the workload pool marked as default pool for its category. This property is defined per workload_pool stanza. Default is 0.
<i>default_pool</i>	Boolean	Specifies a workload pool defined in the search category as the default pool for the search category. 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.

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:dict>
</content>

```

```

        </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
<i>cpu_weight</i>	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.
<i>mem_weight</i>	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.
<i>category</i>	string	Specifies the category in which a pool is created. Can be either "search", "ingest", or "misc".
<i>default_category_pool</i>	Boolean	Specifies the workload pool marked as default pool for its category. This property is defined per workload_pool stanza. Default is 0.
<i>default_pool</i>	Boolean	Specifies a workload pool defined in the search category as the default pool for the search category. <div>                     deprecated parameter retained for backwards compatibility with 7.2.x                 </div>

*ingest\_pool*BooleanSpecifies a workload-pool defined in the ingest category as the default pool for the ingest category.

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=60 -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>

```



```
</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
<i>workload_rule_type</i>	String	<p>Specifies the rule type. Supported values are:</p> <p><code>search_filter</code>: returns admission rules only.</p> <p><code>all</code>: returns both admission rules and workload rules.</p> <div>To list workload rule information only, specify the endpoint URI with optional <code>rule_name</code>, for example <code>services/workloads/rules/rule_name</code>.</div>

### Returned values

Name	Type	Description
<i>predicate</i>	String	Specifies the predicate (condition) that a search must meet for the specified action to be taken.
<i>action</i>	String	Specifies the action taken when a search meets the predicate (condition).
<i>workload_pool</i>	String	Specifies the workload pool associated with the workload rule.
<i>order</i>	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:dict>
    </content>
  </entry>
</feed>
```

```

        </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
<i>name</i>	String	Specifies the name of the workload rule or admission rule.

Name	Type	Description
<i>predicate</i>	String	<p>Specifies a predicate (condition) that must be true for a search to gain access to the workload pool. The syntax is <code>&lt;type&gt;=&lt;value&gt;</code>, with optional AND, OR, NOT, (). For example, <code>app=search AND role=power</code> maps all searches belonging to both the Search app and the power role to the designated workload pool.</p> <p>Valid predicate <code>&lt;type&gt;</code> are <code>app</code>, <code>role</code>, <code>index</code>, <code>user</code>, <code>search_type</code>, <code>search_mode</code>, <code>search_time_range</code>, and <code>runtime</code>. For valid predicate type values, see Predicate type values in the <i>Workload Management</i> manual.</p> <p>You can only specify one predicate for each workload rule. Multiple predicates are not supported.</p>
<i>action</i>	String	<p>For workload rules: Specifies the action taken when a search meets the specified predicate (condition). Supported actions are <code>alert</code>, <code>move</code> and <code>abort</code>.</p> <p>For admission rules: You must specify <code>filter</code> as the action.</p>
<i>destination</i>	String	Specifies the destination workload pool for the <code>move</code> action.
<i>workload_pool</i>	String	Specifies the workload pool associated with the workload rule.
<i>order</i>	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.
<i>workload_rule_type</i>	String	Supported value: <code>search_filter</code> . 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
<i>workload_rule_type</i>	String	Specifies the rule to delete is an admission rule. Supported value: <i>search_filter</i> .

#### 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
------	------	-------------

Name	Type	Description
<i>workload_pool_base_dir_name</i>	String	Specifies the parent level cgroup for splunk.  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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```

```

<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
<i>workload_pool_base_dir_name</i>	String	Specifies the parent level cgroup for splunk. <div>This setting applies only to systems running non-systemd setups. With systemd, this setting is ignored.</div>

**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
<i>admission_rules_enabled</i>	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:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

```



```

        <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
<i>advanced</i>	Boolean	<i>advanced</i> =1 returns dispatch time for each process running in each search pool.

## Returned values

General information:

Name	Type	Description
<i>default_pool</i>	String	Specifies the workload pool marked as the default pool.
<i>ingest_pool</i>	Number	Specifies the workload pool marked as the ingest pool.
<i>error_message</i>	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.
<i>enabled</i>	Boolean	Specifies whether or not workload management is enabled.
<i>isSupported</i>	Boolean	Specifies whether or not workload management is supported on this machine.
<i>os_build</i>	String	Specifies the operating system build information.
<i>os_extended_name</i>	String	Specifies the extended name of the underlying operating system.
<i>os_name</i>	String	Specifies the name of the underlying operating system.
<i>os_version</i>	String	Specifies the operating system version.

Workload pools:

Name	Type	Description
<i>cpu_weight</i>	Number	Specifies the fraction of the cpu assigned to this pool as a ratio of the total of <i>cpu_weight</i> across all pools. This fraction is then applied to the cpu shares assigned to the parent group.
<i>mem_weight</i>	Number	Specifies the fraction of the memory assigned to this pool as a ratio of the total of <i>mem_weight</i> across all pools. This fraction is then applied to the memory limits assigned to the parent group.

Workload rules:

Name	Type	Description
<i>predicate</i>	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.
<i>workload_pool</i>	String	Specifies the workload pool to associate with the workload rule.
<i>order</i>	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:dict>
    </content>
  </entry>

```

```

<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>

```

---