Splunk® Supported Add-ons
Splunk Add-on for VMware released

Generated: 11/01/2022 2:45 pm

Table of Contents

Overview

About the Splunk Add-on for VMware

Version	4.0.4
Vendor Products	VMware vCenter Server versions 6.5, 6.7, 7.0

The Splunk Add-on for VMware is a collection of add-ons that collect data from VMware vCenters, ESXi Hosts and Virtual Machines. It provides deep operational visibility into granular performance metrics, logs, tasks and events and topology from hosts, virtual machines and virtual centers for use with the Splunk IT Service Intelligence Virtualization Module and the Splunk App for VMware.

Download the Splunk Add-on for VMware from Splunkbase at http://splunkbase.splunk.com/app/3215/.

Discuss the Splunk Add-on for VMware on Splunk Answers at http://answers.splunk.com/answers/app/3215/.

Release notes for Splunk Add-on for VMware

Version 4.0.4 of the Splunk Add-on for VMware was released on 29 Apr 2022.

Version 4.0.4 of Splunk Add-on for VMware only contains "Splunk_TA_vmware" and "SA-Hydra" packages. "SA-VMWIndex", "TA-VMW-FieldExtractions", "Splunk_TA_vcenter", "Splunk_TA_esxilogs" packages that were part of add-on build in its v4.0.2 or below, have been removed from the add-on build and will be published as individual apps on Splunkbase.

What's New

For Version 4.0.4, The Splunk Add-on for VMware is now updated with bug fixes.

Upgrade from version 4.0.2 to 4.0.4

See the steps to upgrade from the Splunk Add-on for VMware from v4.0.2 to v4.0.4. If you are using a version previous to 4.0.2, follow the steps to upgrade to v4.0.2 first.

Upgrade from versions 3.4.6 and earlier

In the release 3.3.2, the `SA-Utils` component has been renamed to `SA-VMNetAppUtils`. It does not change the input and dashboard you configured in Splunk Add-on for VMware and Splunk App for VMware.

In the release 3.4.2, a new component, `SA-VMWIndex` has been added to the Splunk Add-on for VMware package. This component contains the indexes.conf which has the definitions of all the indexes [vmware-perf, vmware-inv, vmware-taskevent, vmware-vclog, vmware-esxilog]. The indexes.conf will be removed from all the components of VMware Add-on as these have been added to `SA-VMWIndex`.

In the release 3.4.3, a new component, `TA-VMW-FieldExtractions` has been added to the Splunk Add-on for VMware package. This component contains the search time knowledge objects. The search time knowledge objects have been removed from `Splunk_TA_vmware` .

See the upgrade section of the Splunk App for VMware manual for the detailed procedures.

Note: Splunk recommend you backup your existing deployment before upgrade.
See "Back up configuration information" in the *Admin Manual* and "Back up indexed data" in the *Managing Indexers and Clusters Manual*

Fixed Issues

This version of the Splunk Add-on for VMware has the following reported fixed issues. If no issues appear below, no issues have yet been reported.

Known Issues

This version of the Splunk Add-on for VMware has the following reported known issues and workarounds. If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2021-08-05	VMW-6236	Incorrect value for Cluster performance metrics due to aggregation mechanism on vCenter side.
2021-06-09	VMW-6165	Drill-down not working in Event viewer panels in Hydra Framework in Splunk 8.2.0,8.2.1
2020-09-30	VMW-5802	No data collection occurs when the DCN is configured with more than 8 worker processes on Splunk version 8.x.
2019-10-11	VMW-5269	Collection configuration page doesn't get loaded in Internet Explorer browser
2019-09-19	VMW-5240	Gaps and negative values in VMware Host/VM Performance data at random time samples
2019-09-19	VMW-5239	Duplication in performance data for random sampling time
2019-06-19	VMW-5134	Field changeset is having value "null" in inventory data
2018-04-25	VMW-4848	DCN collection worker failures - vmodl.query.PropertyCollector:session exceptions.

Release history for Splunk Add-on for VMware

Latest release

These features apply to Splunk Add-on for VMware version 4.0.4. For compatibility information, see Installation and configuration overview for the Splunk Add-on for VMware in the Splunk Add-on.

New feature or enhancement	Description
Some minor bug fixes	Updated key for syslog stanza
Added triggers stanza for custom configuration files	To avoid unnecessary restarts of the Splunk platform, updated `app.conf` file with a [triggers] stanza and a `reload` setting for custom configuration file

Version 4.0.3

These features apply to Splunk Add-on for VMware version 4.0.3. For compatibility information, see Installation and configuration overview for the Splunk Add-on for VMware in the Splunk Add-on.

Self-Service Installation Compatibility

The Splunk Add-on for VMware is now available for self-service installation in cloud environments. The following packages have been removed from the add-on package and published as individual Splunkbase add-ons to support self-service installation in cloud environments:

Package	Splunkbase Add-on	Version
SA-VMWIndex	Splunk Add-on for VMware Indexes	4.0.3
TA-VMW-FieldExtractions	Splunk Add-on for VMware Extractions	4.0.3
Splunk_TA_esxilogs	Splunk Add-on for VMware ESXi Logs	4.2.1
Splunk_TA_vcenter	Splunk Add-on for vCenter Logs	4.2.1

jQuery 3.5 Compatibility

The Splunk Add-on for VMware is now updated to use jQuery v3.5.0. The add-on uses jQuery v3.5 in the Splunk version 8.2 or later. This makes the add-on more secure by fixing known cross-site scripting (XSS) related vulnerabilities as well as vulnerabilities created by object prototype pollution.

Version 4.0.2

This version of the Splunk Add-on for VMware doesn't contain biased terms such as master, slave, blacklist, and whitelist have been replaced with appropriate non-biased terms. The occurrences of biased terms that are Splunk platform references or present in the third-party library have not been removed. The following table contains the parameters from the ta_vmware_collection.conf file present in the Splunk_TA_vmware package that has been renamed to remove biased language:

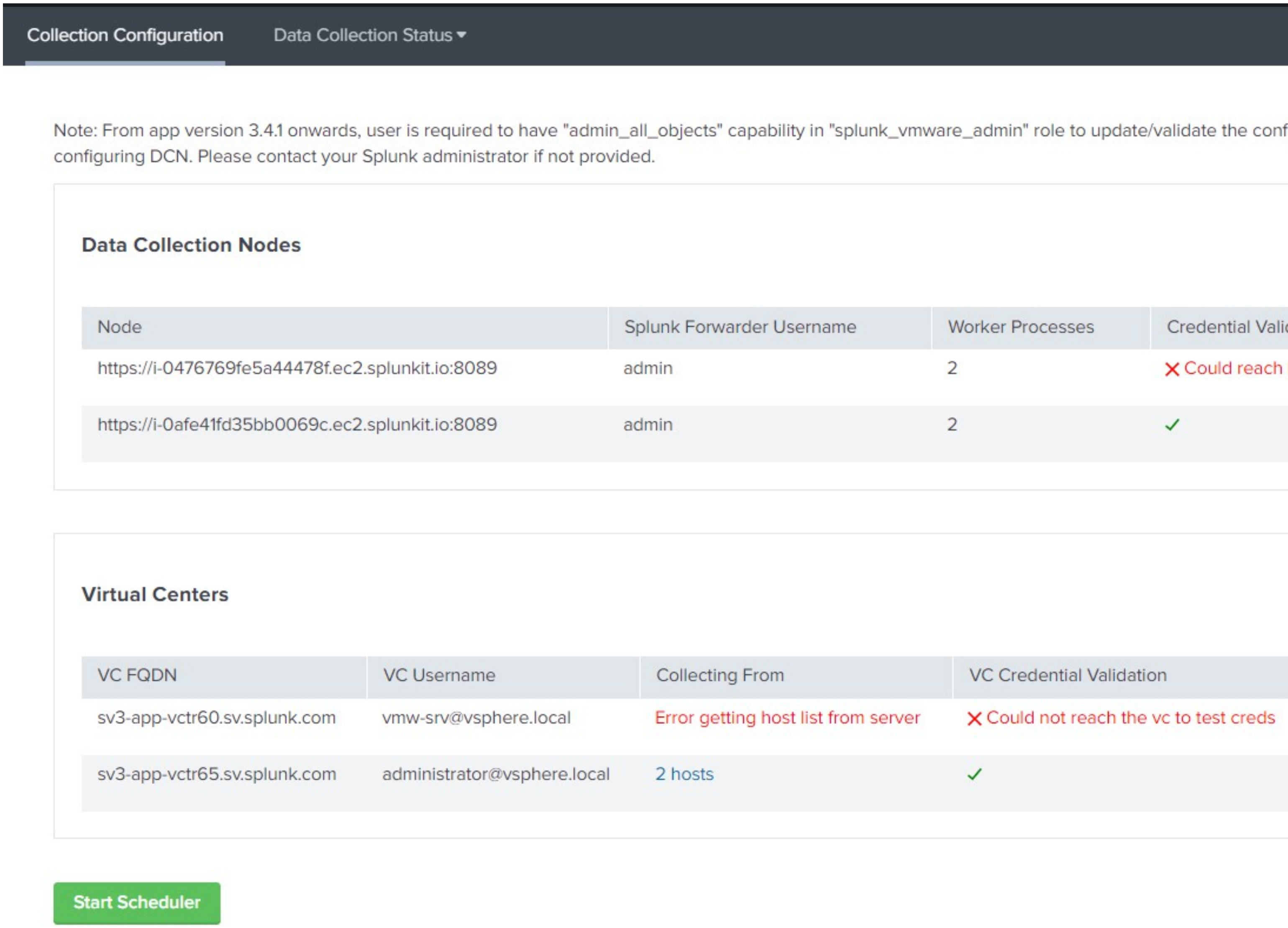
Parameter name in Splunk Add-on for VMware version 4.0.1	Parameter name in Splunk Add-on for VMware version 4.0.2
managed_host_whitelist	managed_host_includelist
managed_host_blacklist	managed_host_excludelist
vm_metric_whitelist	vm_metric_allowlist
vm_metric_blacklist	vm_metric_denylist
host_metric_whitelist	host_metric_allowlist
host_metric_blacklist	host_metric_denylist
cluster_metric_whitelist	cluster_metric_allowlist
cluster_metric_blacklist	cluster_metric_denylist
rp_metric_whitelist	rp_metric_allowlist
rp_metric_blacklist	rp_metric_denylist
vm_instance_whitelist	vm_instance_allowlist

Parameter name in Splunk Add-on for VMware version 4.0.1	Parameter name in Splunk Add-on for VMware version 4.0.2
vm_instance_blacklist	vm_instance_denylist
host_instance_whitelist	host_instance_allowlist
host_instance_blacklist	host_instance_denylist
cluster_instance_whitelist	cluster_instance_allowlist
cluster_instance_blacklist	cluster_instance_denylist
rp_instance_whitelist	rp_instance_allowlist
rp_instance_blacklist	rp_instance_denylist
perf_entity_blacklist	perf_entity_denylist

- In the vCenter configuration, you'll see inputs for "Host Includelist Regex" and "Host Excludelist Regex" instead of "Host Whitelist Regex" and "Host Blacklist Regex", to allow or block the performance data collection of certain hosts present in the vCenter server.
- In the Data Collection Preference, you'll see inputs for "Metric Allowlist" and "Metric Denylist" instead of "Metric Whitelist" and "Metric Blacklist", to allow or block the data collection of specific metrics.

Version 3.4.6

Version 3.4.6 of the Splunk Add-on for VMware includes a redesigned Collection Configuration page for the collection of Data Collection Node and Virtual Center data.



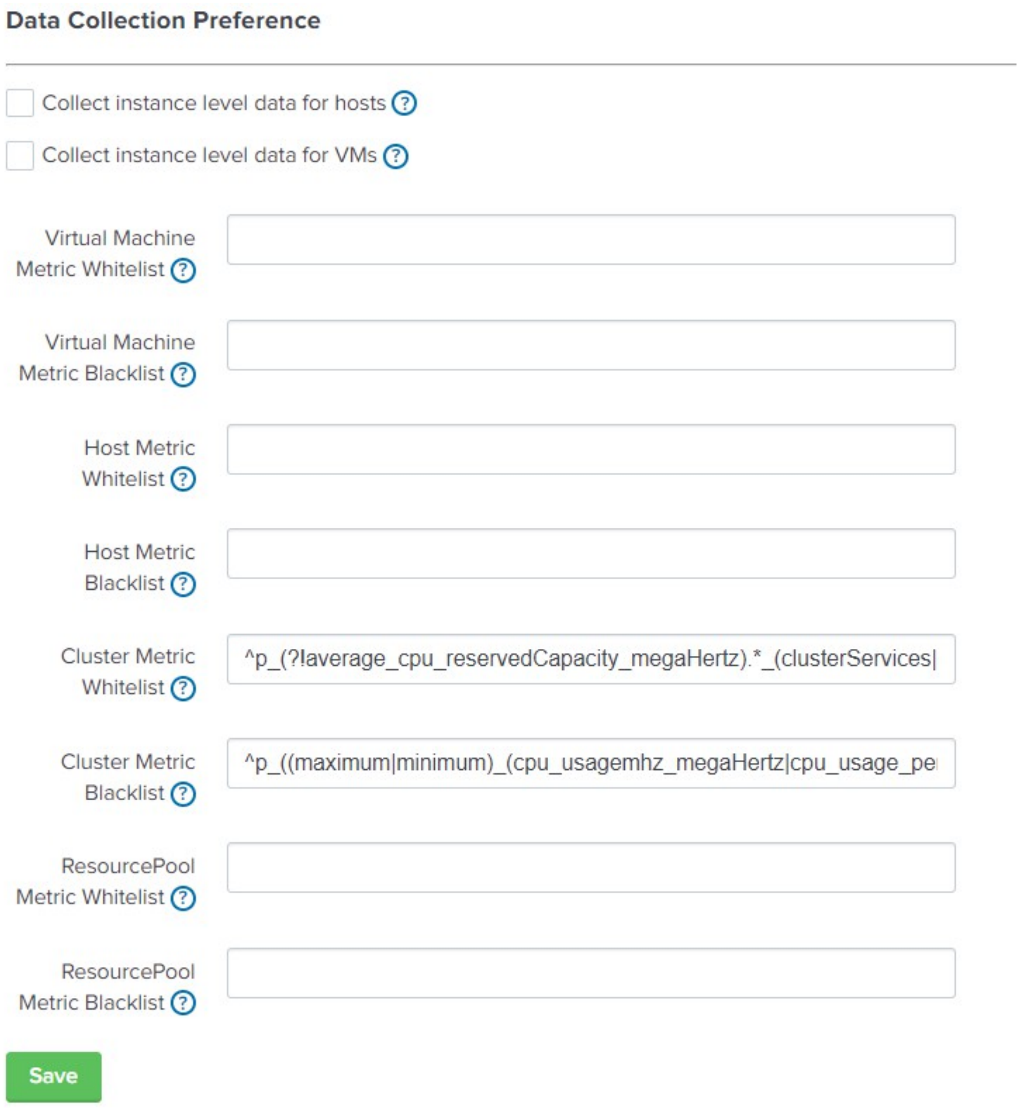
Note: From app version 3.4.1 onwards, user is required to have "admin_all_objects" capability in "splunk_vmware_admin" role to update/validate the conf configuring DCN. Please contact your Splunk administrator if not provided.

Data Collection Nodes

Node	Splunk Forwarder Username	Worker Processes	Credential Vali
https://i-0476769fe5a44478f.ec2.splunkit.io:8089	admin	2	✕ Could reach
https://i-0afe41fd35bb0069c.ec2.splunkit.io:8089	admin	2	✓

Virtual Centers

VC FQDN	VC Username	Collecting From	VC Credential Validation
sv3-app-vctr60.sv.splunk.com	vmw-srv@vsphere.local	Error getting host list from server	✕ Could not reach the vc to test creds
sv3-app-vctr65.sv.splunk.com	administrator@vsphere.local	2 hosts	✓

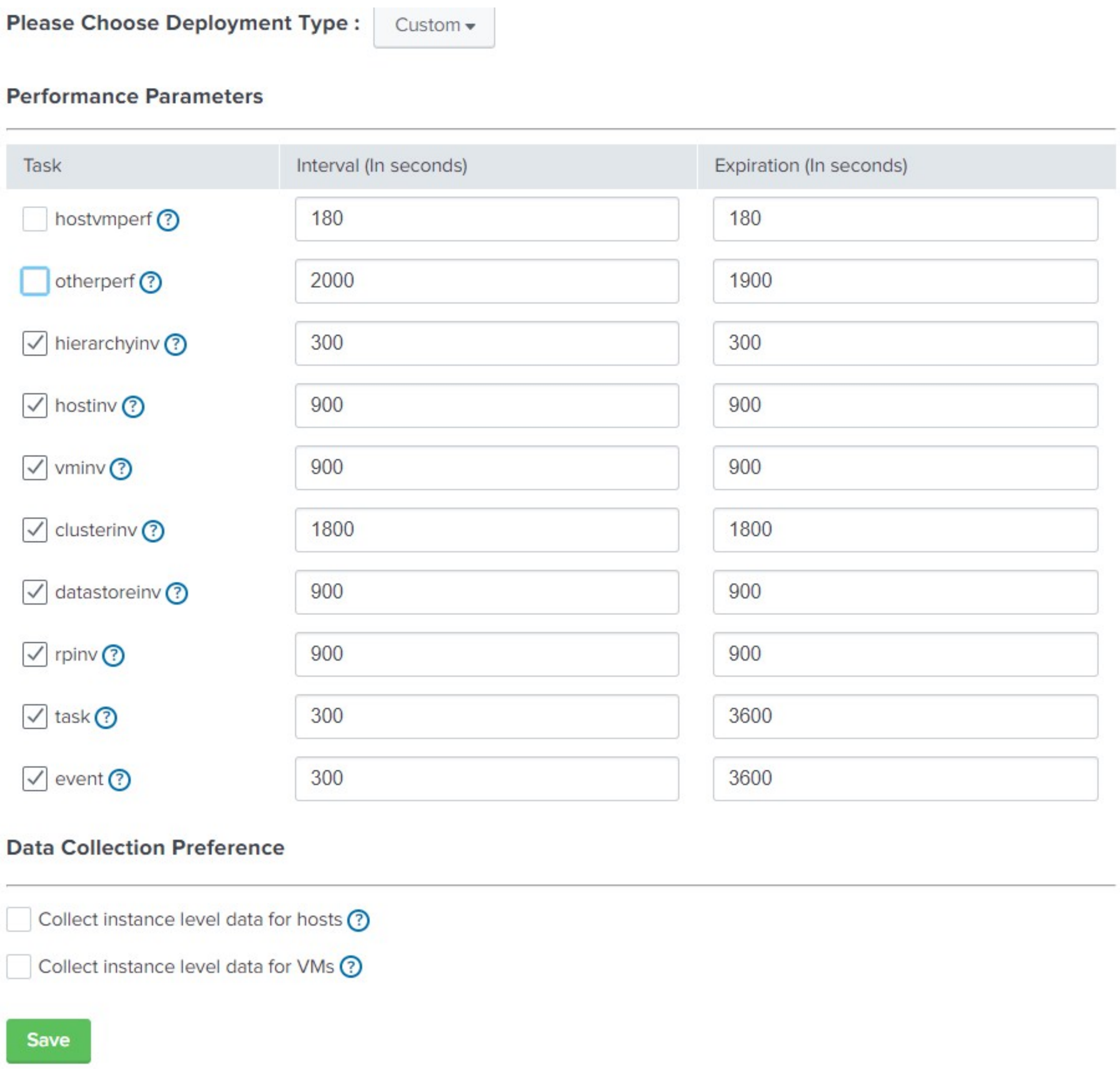


Data Collection Preference

□ Collect instance level data for hosts

□ Collect instance level data for VMs

Virtual Machine Metric Whitelist	
Virtual Machine Metric Blacklist	
Host Metric Whitelist	
Host Metric Blacklist	
Cluster Metric Whitelist	^p_(?!average_cpu_reservedCapacity_megaHertz).*_(clusterServices|
Cluster Metric Blacklist	^p_((maximum|minimum)_(cpu_usagemhz_megaHertz|cpu_usage_pe
ResourcePool Metric Whitelist	
ResourcePool Metric Blacklist	



Please Choose Deployment Type : Custom ▾

Performance Parameters

Task	Interval (In seconds)	Expiration (In seconds)
□ hostvmperf ?	180	180
□ otherperf ?	2000	1900
☑ hierarchyinv ?	300	300
☑ hostinv ?	900	900
☑ vminv ?	900	900
☑ clusterinv ?	1800	1800
☑ datastoreinv ?	900	900
☑ rpinv ?	900	900
☑ task ?	300	3600
☑ event ?	300	3600

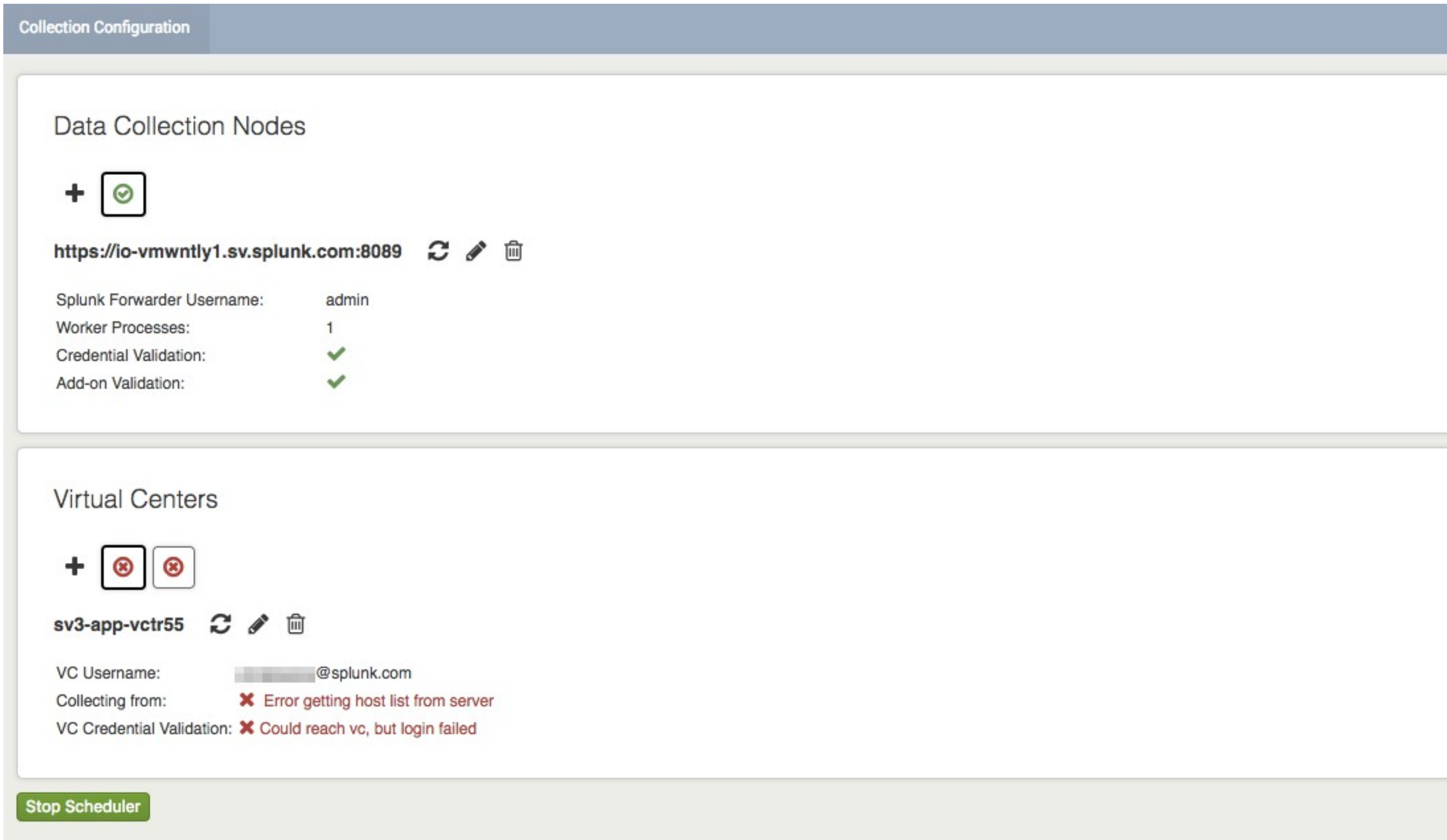
Data Collection Preference

□ Collect instance level data for hosts ?

□ Collect instance level data for VMs ?

Version 3.4.0

Version 3.4.0 of the Splunk Add-on for VMware includes an updated **Collection Configuration** page for the collection of Data Collection Node and Virtual Center data.



Data Collection Nodes

https://io-vmwntly1.sv.splunk.com:8089

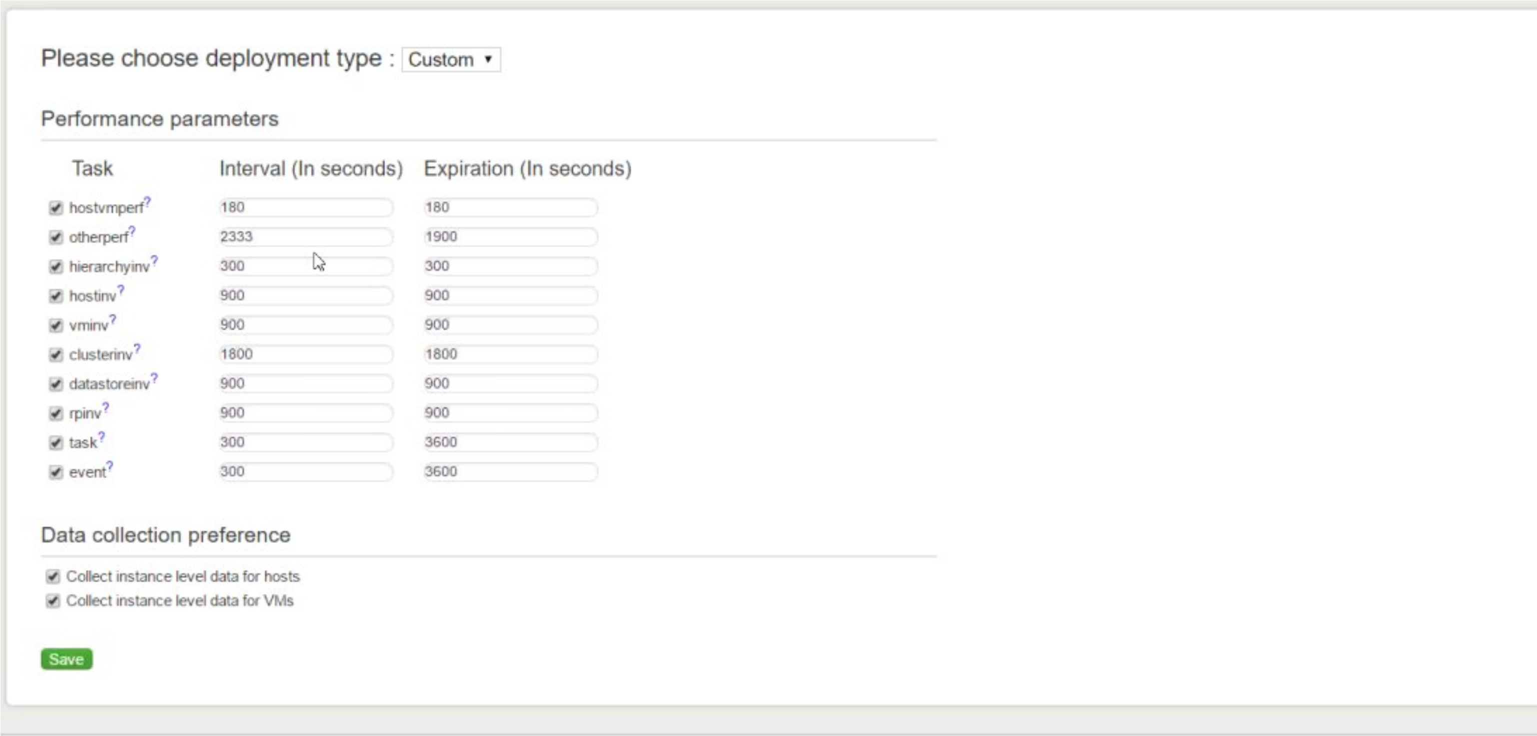
Splunk Forwarder Username: admin
Worker Processes: 1
Credential Validation: ✓
Add-on Validation: ✓

Virtual Centers

sv3-app-vctr55

VC Username: [redacted]@splunk.com
Collecting from: ✖ Error getting host list from server
VC Credential Validation: ✖ Could reach vc, but login failed

The **Collection Configuration** page can now be used to set interval and expiration times for the performance parameters of the Splunk Add-on for VMware.



Please choose deployment type : Custom ▾

Performance parameters

Task	Interval (In seconds)	Expiration (In seconds)
☑ hostvmperf?	180	180
☑ otherperf?	2333	1900
☑ hierarchyinv?	300	300
☑ hostinv?	900	900
☑ vminv?	900	900
☑ clusterinv?	1800	1800
☑ datastoreinv?	900	900
☑ rpinv?	900	900
☑ task?	300	3600
☑ event?	300	3600

Data collection preference

☑ Collect instance level data for hosts
☑ Collect instance level data for VMs

This information can also be adjusted using `ta_vmware_collection.conf` in `$SPLUNK_HOME/etc/apps/TA_vmware/local/`.

Upgrade from versions 3.3.1 and earlier

In the release 3.3.2, the `SA-Utils` component has been renamed to `SA-VMNetAppUtils`. It does not change the input and dashboard you configured in Splunk Add-on for VMware and Splunk App for VMware.

In the release 3.4.2, a new component, `SA-VMWIndex` has been added to the Splunk Add-on for VMware package. This component contains the indexes.conf which has the definitions of all the indexes [vmware-perf, vmware-inv, vmware-taskevent, vmware-vclog, vmware-esxilog]. The indexes.conf will be removed from all the components of VMware Add-on as these have been added to `SA-VMWIndex`.

In the release 3.4.3, a new component, TA-VMW-FieldExtractions has been added to the Splunk Add-on for VMware package. This component contains the search time knowledge objects. The search time knowledge objects have been removed from Splunk_TA_vmware.

See the upgrade section of the Splunk App for VMware manual for the detailed procedures.

Note: Splunk recommend you backup your existing deployment before upgrade.
See "Back up configuration information" in the *Admin Manual* and "Back up indexed data" in the *Managing Indexers and Clusters Manual*

Fixed Issues

Date resolved	Issue number	Description
2017-04-07	VMW-4484	Support of all ESXi logs format - Correct the sourcetype and field extraction regex (Splunk_TA_esxilogs)
2017-03-30	VMW-4428	Splunk_TA_vcenter Add-on field extraction
2017-03-17	VMW-4320, NETAPP-809	Certification Validation is disabled
2017-03-03	VMW-4437	Splunk unable to connect to some vcenters - vcenters being marked as dead
2017-02-28	VMW-4501, NETAPP-800	Deprecated supportSSLV3Only = <bool> still being used in the latest version of vmware
2017-02-08	VMW-4449	Remove logging of Splunk session keys
2017-02-06	VMW-4380	Splunk DCN making excessive DNS queries

Known Issues

Date filed	Issue number	Description
2019-01-07	VMW-4960	vpxd.stats.maxQueryMetrics error prevents data collection from vCenters
2018-08-27	VMW-4907	Licence Issue for Partner NFR
2018-04-10	VMW-4840	Scrolling issue in Collection Configuration page
2018-02-15	VMW-4825, VMW-4795	Security Scan Failure for port 8008 SA-Hydra for accepting aNULL Cipher Suite
2017-12-11	VMW-4794	Performance fields are not extracted from vmware:perf:vflashModule sourcetype
2017-08-18	VMW-4658	source=VMPerf:VirtualMachine event missing while one of the vCenters is unreachable
2017-05-19	VMW-4597	Not getting "vmware:vclog:vws" sourcetype in vCenter v6.5.
2017-05-19	VMW-4598	"opId" field is not getting extracted properly for few events from "vmware:vclog:vpxd" source type.

Installation and Configuration

Hardware and software requirements for the Splunk Add-on for VMware

Current add-on version	Supported versions of VMware vCenter Server	Supported versions of Splunk Enterprise
4.0.4	6.5, 6.7, 7.0	8.0.x, 8.1.x, 8.2.x, 9.0.0

All of the system requirements for the Splunk platform apply for the Splunk software that you use to run this add-on. The Splunk Add-on for VMware does not support scheduler and Data Collection Node functions on Windows operating systems. Linux or UNIX are required. When deploying the VMware add-on into a Windows-based Splunk environment, deploy Linux-based virtual appliances from the Splunk-provided OVA image for both scheduler and data collection node roles.

- For Splunk Enterprise system requirements: see System Requirements in the Splunk Enterprise *Installation Manual*.
- For Splunk Light system requirements: see System Requirements in the Splunk Light *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

> Data Collection Node supports SSL certificate with encrypted private key for Splunk versions 7.3.3 and later, except for Splunk version 8.0.0

Browser support

The Splunk Add-on for VMware supports the the latest version of the following browsers:

- Firefox
- Safari
- Chrome

Data volume requirements

In a typical environment, approximately 250 MB and 350 MB of data can be collected per host per day from your environment. This number varies depending on the volume of log data you collect, and the number of virtual machines that reside on a host. See the information below for further details.

Collected data type	Data volume
Total vCenter logs	15 MB of data per host per day per vCenter. For example, 750MB in a 50 host environment.
ESXi host logs	185 MB of data per host per day. (In a typical environment this number can range from 135MB to 235M of data, but it can vary widely depending on your environment).
Total API data per host	10 MB of data per host per day.
Total API data per virtual machine	3 MB of data per day.

Compatibility with pre-requisite add-on packages

The packages SA-VMWIndex, TA-VMW-FieldExtractions, Splunk_TA_esxilogs, Splunk_TA_vcenter that were included in add-on v4.0.2 or previous are now shipped as individual Splunkbase add-ons as of v4.0.3. Please refer to the table for the add-on version compatibility with the new packages. The given add-ons are pre-requisites for the Splunk Add-on For VMware. Below is the purpose of each add-ons:

1. Splunk Add-on for VMware Indexes (contains SA-VMWIndex package): Contains the definition of indexes that are used by Splunk Add-on for VMware, Splunk Add-on for vCenter Logs, and Splunk Add-on for VMware ESXi Logs.
2. Splunk Add-on for VMware Extractions (contains TA-VMW-FieldExtractions package): Contains the field extractions for the data ingested by Splunk Add-on for VMware and search-time extractions used in Splunk App for VMware.
3. Splunk Add-on for VMware ESXi logs (contains Splunk_TA_esxilogs package): Contains inputs, search-time and Index-time extractions for the collection, parsing, and ingestion of VMware ESXi logs in the Splunk environment.
4. Splunk Add-on for vCenter Logs (contains Splunk_TA_vcenter package): Contains the inputs, search-time and index-time extractions for the collection, parsing, and ingestion of vCenter logs in the Splunk environment.

Splunk Add-on for VMware version	Compatible Splunk Add-on for VMware Indexes version	Compatible Splunk Add-on for VMware Extractions version	Compatible Splunk Add-on for VMware ESXi Logs version	Compatible Splunk Add-on for VMware vCenter Logs version
4.0.3	4.0.3	4.0.3	4.2.1	4.2.1
4.0.4	4.0.3	4.0.3	4.2.1	4.2.1

Version compatibility

vCenter versions 5.0 to 6.0 are EOL (End of Life).

Compatible Splunk platform version	Compatible Splunk Add-on for VMware version	Compatible vCenter version	Compatible vSphere version	Compatible ESXi version	Compatible SA-Hydra version	Compatible SA-VMWNetAppUtils version
6.3 to 6.5	3.3.1	5.0 to 6.0	4.1, 5.0, 5.0 Update 1, 5.1, 5.5, 5.5a, 6.0	4.1, 5.0, 5.0 Update 1, 5.1, 5.5 on 64-bit x86 CPUs, 5.5 update 1 and above.	4.0.2 and above	3.5.0, 3.7.0
6.3 to 6.5	3.3.2	5.0,6.0,6.5	4.1, 5.0, 5.0 Update 1, 5.1, 5.5, 5.5a, 6.0	4.1, 5.0, 5.0 Update 1, 5.1, 5.5 on 64-bit x86 CPUs, 5.5 update 1 and above.	4.0.4	1.0.0 (Version 3.3.2 replaces `SA-Utils` with `SA-VMNetAppUtils`
6.4 to 6.6	3.4.0	5.5,6.0,6.5	5.5,6.0,6.5	5.5,6.0,6.5	4.0.5	1.0.1
6.5 to 7.0	3.4.1	5.5,6.0,6.5	5.5,6.0,6.5	5.5,6.0,6.5	4.0.6	1.0.2
6.6 to 7.1	3.4.2	5.5,6.0,6.5	5.5,6.0,6.5	5.5,6.0,6.5	4.0.7	1.0.3

Compatible Splunk platform version	Compatible Splunk Add-on for VMware version	Compatible vCenter version	Compatible vSphere version	Compatible ESXi version	Compatible SA-Hydra version	Compatible SA-VMWNetAppUtils version
7.0 to 7.2	3.4.3	5.5,6.0,6.5,6.7	5.5,6.0,6.5,6.7	5.5,6.0,6.5,6.7	4.0.8	1.0.4
7.0.0 to 7.2.1	3.4.4	5.5,6.0,6.5,6.7	5.5,6.0,6.5,6.7	5.5,6.0,6.5,6.7	4.0.8	1.0.5
7.1.0 to 7.3.1	3.4.5	6.0,6.5,6.7	6.0,6.5,6.7	6.0,6.5,6.7	4.0.9	1.0.5
7.2.x to 8.0.0	3.4.6	6.0, 6.5, 6.7	6.0, 6.5, 6.7	6.0, 6.5, 6.7	4.1.0	1.0.5
7.2.x to 8.0.x	3.4.7	6.0, 6.5, 6.7	6.0, 6.5, 6.7	6.0, 6.5, 6.7	4.1.1	N/A
7.2.x to 8.0.x	4.0.0	6.0, 6.5, 6.7	6.0, 6.5, 6.7	6.0, 6.5, 6.7	4.1.2	N/A
7.2.x to 8.1.0	4.0.1	6.0, 6.5, 6.7	6.0, 6.5, 6.7	6.0, 6.5, 6.7	4.1.3	N/A
7.3.x to 8.2.0	4.0.2	6.0, 6.5, 6.7	6.0, 6.5, 6.7	6.0, 6.5, 6.7	4.1.5	N/A
8.0.x to 8.2.0	4.0.3	6.5, 6.7, 7.0	6.5, 6.7, 7.0	6.5, 6.7, 7.0	4.1,7	N/A
8.0.x to 9.0.0	4.0.4	6.5, 6.7, 7.0	6.5, 6.7, 7.0	6.5, 6.7, 7.0	4.1.8	N/A

Requirements for installing Splunk Add-on for VMware with other add-ons

The following requirements apply to installing Splunk Add-on for VMware and Splunk Add-on for VMware Metrics in the same environment:

Splunk Add-on for VMware Metrics version	Splunk Add-on for VMware version	Can DCS be installed on the same machine?	Can DCN be installed on the same machine?
4.0.0 or later	3.4.7	Yes	No
1.0.0, 1.1.0 or 1.1.1 (Splunk VMware Add-on for ITSI)	3.4.7	No	No

The following requirements apply to installing Splunk Add-on for NetApp ONTAP and Splunk Add-on for VMware in the same environment:

Splunk Add-on for NetApp ONTAP version	Splunk Add-on for VMware version	Can DCS be installed on the same machine?	Can DCN be installed on the same machine?
3.0.0 or later	3.4.6 or later	No	No
2.1.91 or before	3.4.5 or before	Yes	No

Installation and configuration overview for the Splunk Add-on for VMware

The Splunk Add-on for VMware package contains the following components:

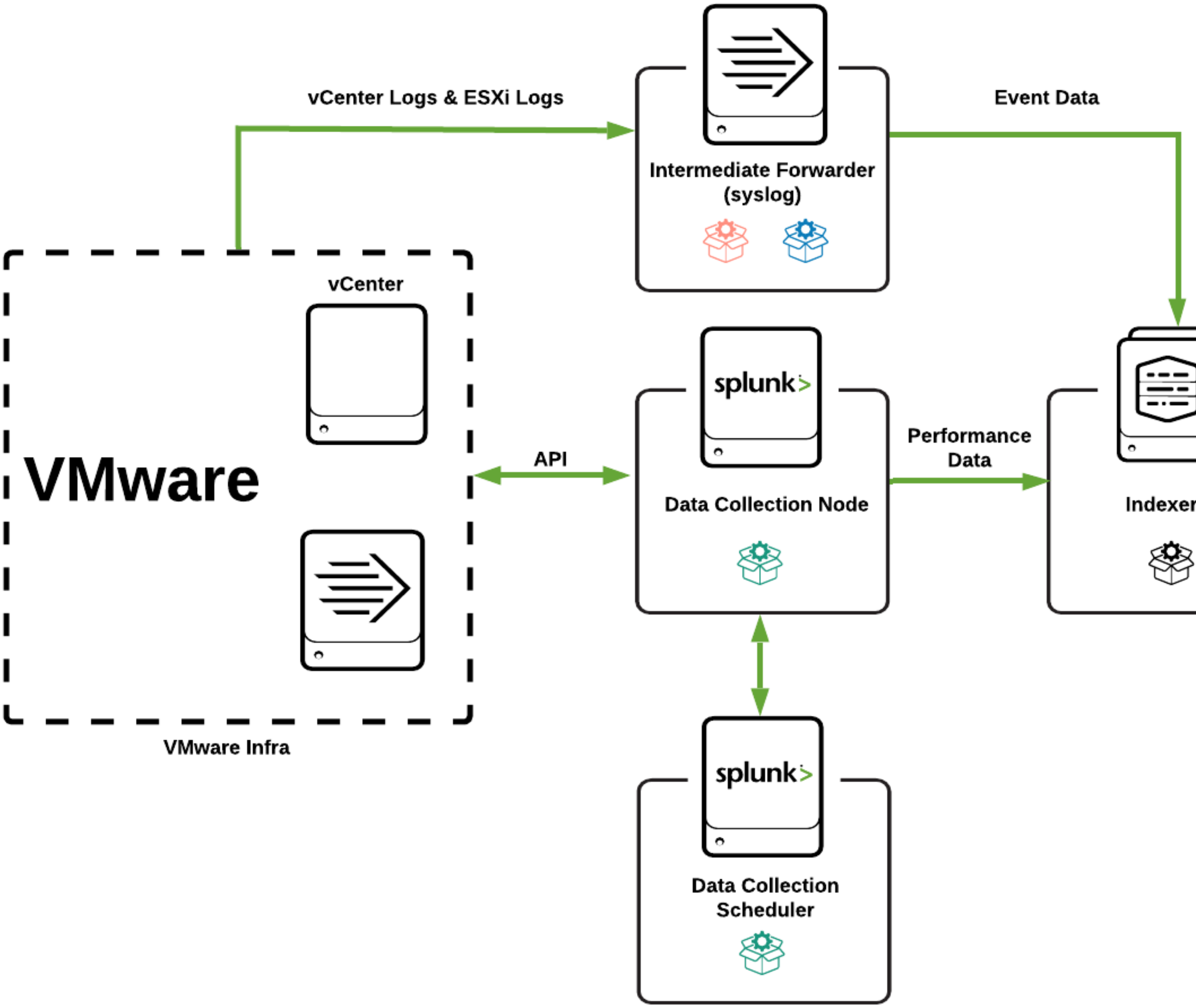
- **SA-Hydra** - Collects API based data from vCenter. It schedules jobs from the Search Head and runs the worker processes on each data collection node.
- **Splunk_TA_vmware** - Contains the python based API data collection engine and collects data from VMWare environment. Also provides search-time tagging of VMware data.

The Splunk Add-on for VMware contains the following functions:

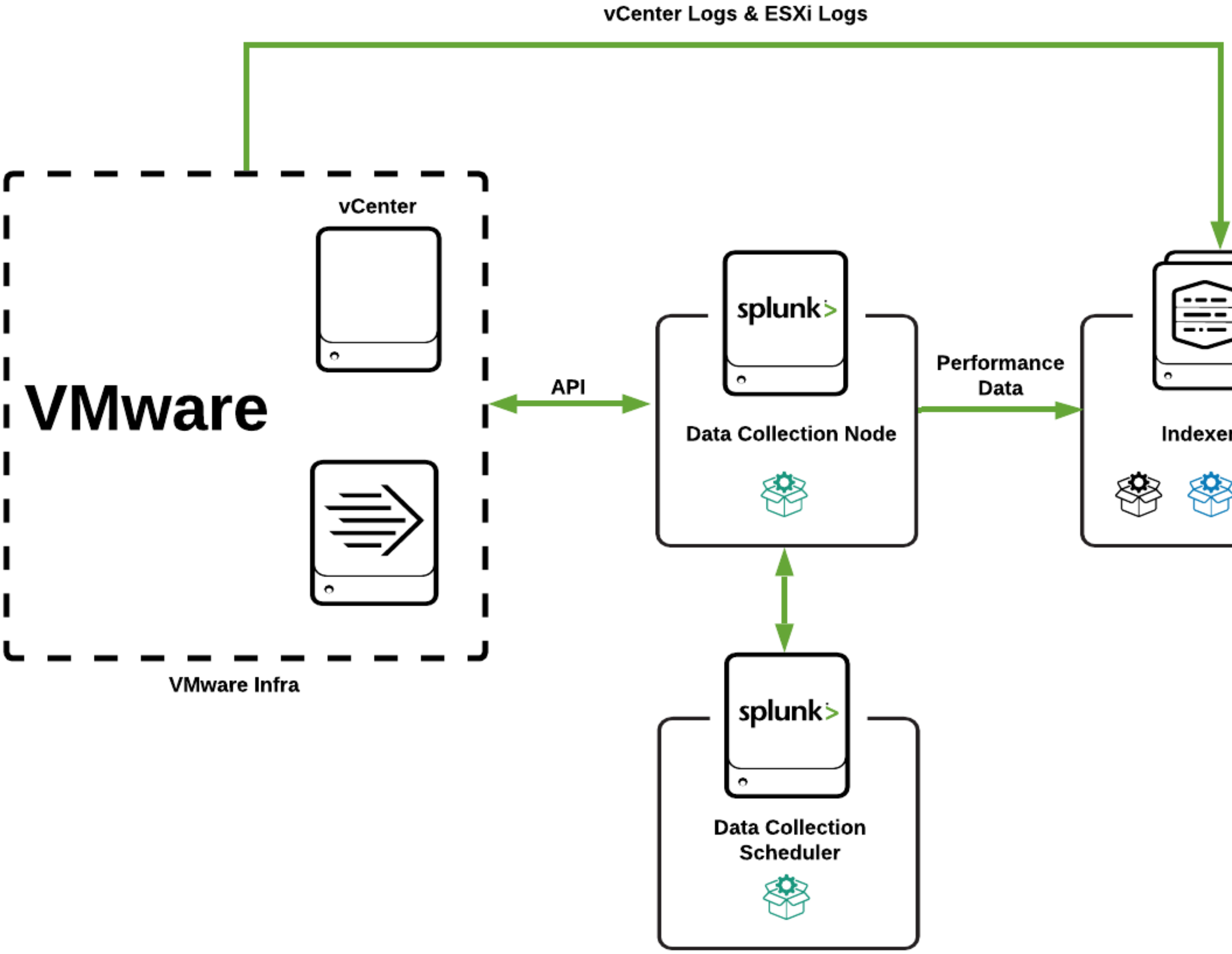
- **Scheduler** - Previously held by the Splunk App for VMware, the scheduler performs job distribution and load balancing for your distributed Splunk platform deployment.
- Python script `splunk_for_vmware_setup.py` that collects DCN details, such as DCN URI, username, and password information from the **Collection Configuration** page of the Splunk Add-on for VMware and sends them to SA-Hydra.

Layout for on-premises deployment

The below image outlines the best-practice, full installation of the Splunk Add-on for VMware on a distributed deployment.


vCenter Logs & ESXi Logs
Intermediate Forwarder
(syslog)
Event Data
vCenter
VMware
API
Data Collection Node
Performance
Data
Indexer
VMware Infra
Data Collection
Scheduler

The below image outlines an alternative, full installation of the Splunk Add-on for VMware on a distributed deployment.



On-premises deployment of the Splunk Add-on for VMware

See the table below to see which component goes on which part of your Splunk deployment.

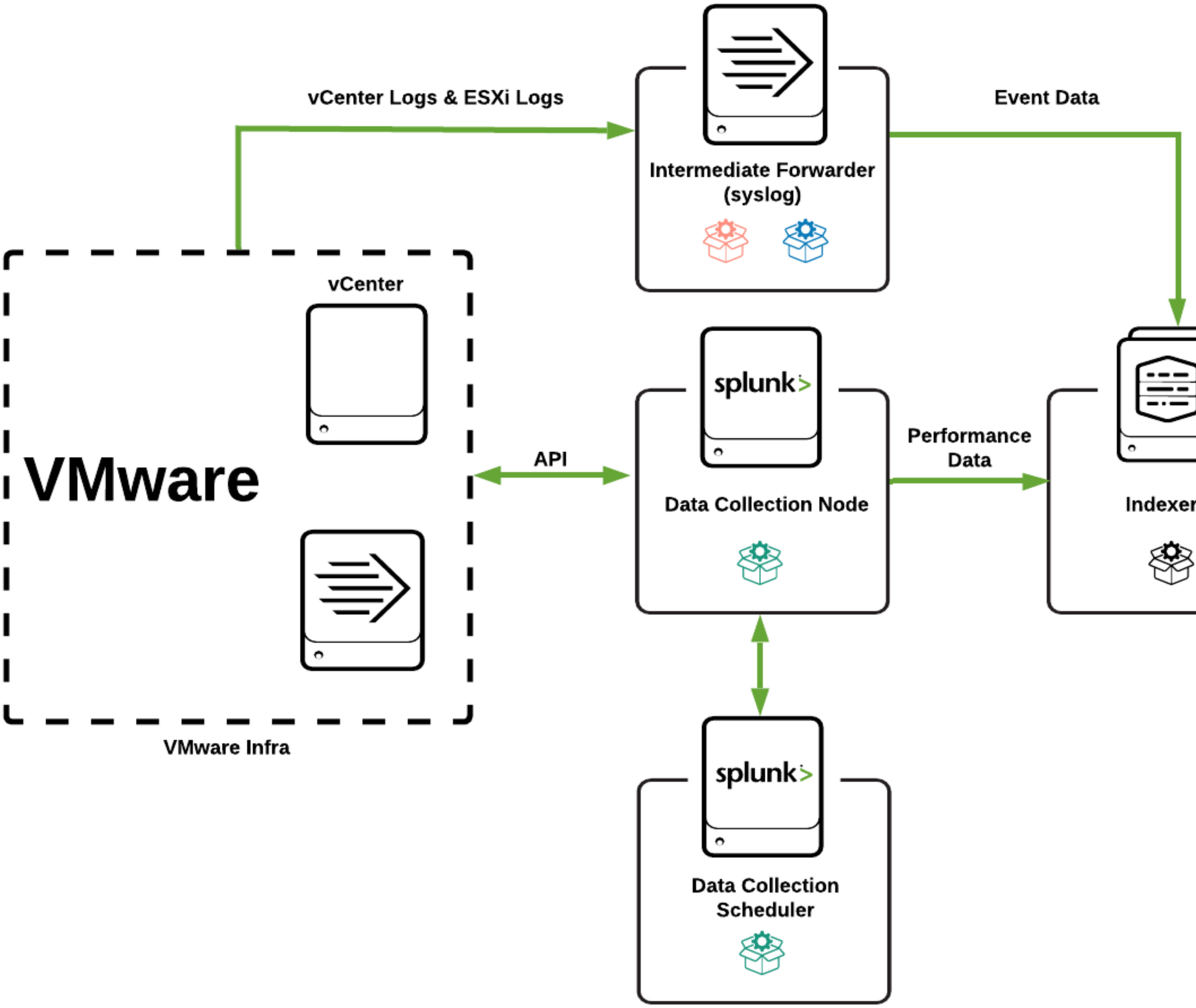
Splunkbase Add-on	Component	Search head	Scheduler (DCS)	Indexer	Data Collection Node (DCN)	Dedicated ESXi log forwarder	Dedicated vCenter log forwarder
Splunk Add-on for VMware	Splunk_TA_vmware SA-Hydra		X		X		
Splunk Add-on for ESXi Logs	Splunk_TA_esxilogs	X		X		X	
Splunk Add-on for vCenter Logs	Splunk_TA_vcenter	X		X	Optional*		X
Splunk Add-on for VMware Indexes	SA-VMWIndex			X			
Splunk Add-on for VMware Extractions	TA-VMW-FieldExtractions	X					

(*)Depending on your specific configuration, you might also need Splunk_TA_vcenter to collect VCenter data.

Forwarding vCenter application logs to Syslog, an intermediate forwarder, or directly to a Splunk indexer is supported from 6.x to 7.0 versions of vCenter Server.

Layout for cloud deployment

The below image outlines a full installation of the Splunk Add-on for VMware on a cloud deployment.


vCenter Logs & ESXi Logs
Event Data
Intermediate Forwarder (syslog)
vCenter
VMware
API
splunk>
Data Collection Node
Performance Data
Indexer
VMware Infra
splunk>
Data Collection Scheduler

Cloud deployment of the Splunk Add-on for VMware

See the table below to see which component goes on which part of your Splunk Cloud deployment.

Splunkbase Add-on	Component	Search head	Scheduler (DCS)	Indexer	Data Collection Node (DCN)	Dedicated ESXi log forwarder	Dedicated vCenter log forwarder
Splunk Add-on for VMware	Splunk_TA_vmware SA-Hydra		X		X		
Splunk Add-on for ESXi Logs	Splunk_TA_esxilogs	X				X	
Splunk Add-on for vCenter Logs	Splunk_TA_vcenter	X					X
Splunk Add-on for VMware Indexes	SA-VMWIndex			X			
Splunk Add-on for VMware Extractions	TA-VMW-FieldExtractions	X					

Set up your system for the Splunk Add-on for VMware

Plan your installation in a test environment

Install the Splunk Add-on for VMware and its prerequisites into a test environment before you install it in a production environment. This way you can work out any issues that you might encounter in your deployment.

After you install the Splunk Add-on for VMware and its prerequisites in your test environment, scale the deployment with more advanced Splunk platform deployment features, such as search head clustering and indexer clustering.

If you don't have access to a test environment, limit the number of hosts and vCenter Servers you use when you first deploy the app and then add complexity after your initial setup is successful.

Splunk Add-on for VMware sample test environment

Use the following test environment size:

- One vCenter Server that supports 40 or fewer ESXi hosts.
- One instance of Splunk Enterprise with one search head and one indexer. See Platform and hardware requirements for Splunk Enterprise versions that support the Splunk Add-on for VMware.
- One Data Collection Node (DCN).

See Install the Splunk OVA for VMware Metrics in your virtual environment section in *Splunk OVA for VMware Metrics* for DCN system requirements.

Create your data collection nodes

Data Collection Nodes (DCNs) are custom Splunk forwarders for connecting, polling data from and enriching data from your VMWare vCenters and forwarding it back to your indexers. See Install the Splunk OVA for VMware Metrics in your virtual environment for more information.

In your test environment, deploy the DCN using the configured Splunk OVA to collect vCenter Server API data. With the following specifications, one data collection node can collect from 40 ESXi hosts or fewer, with a ratio of 25 to 30 virtual machines per host. The default virtual machine included with the Splunk Add-on for VMware is set with this configuration.

- Four cores. Four vCPUs or two vCPUs with two cores with a reservation of 2GHz
- 6GB memory with a reservation of 1GB
- 10-12GB of disk space

Optionally, you can set up a syslog collector when you install and configure Splunk Add-on for VMware. This action is not required for a working VMware app deployment. See the Configure the Splunk Add-on for VMware to collect data section of the Splunk Add-on for VMware to learn more about syslog collection.

See the Deploy OVA to create a Data Collection Node section of the Splunk OVA for VMware and NetApp to learn more.

Set up a vCenter Server user account

Obtain VMware vCenter Server account credentials for each vCenter Server system.

These credentials allow the Splunk Add-on for VMware read-only API access to the appropriate metrics on each vCenter Server system in the environment. the Splunk Add-on for VMware uses the credentials when the DCN polls vCenter Server systems for performance, hierarchy, inventory, task, and event data. These credentials are required for DCN configuration. You can use existing vCenter Server account credentials, or create a new account for Splunk Add-on for VMware to access the vCenter Server data.

Permissions in vSphere

Splunk Add-on for VMware must use valid vCenter Server service credentials to gain read-only access to vCenter Server systems using API calls. The account's vSphere role determines access privileges.

The following sections list the permissions for the vCenter server roles for all of the VMware versions that Splunk App for VMware supports.

Permissions to use your own syslog server

Best practice dictates that use your own syslog server, and that you install a Splunk Enterprise forwarder on the server to forward syslog data. Use these permissions to collect data from the ESXi hosts using your own syslog server. These system-defined privileges are always present for user-defined roles.

Permission
System.Anonymous
System.Read
System.View

Permissions to use an intermediate forwarder

Use these permissions if you configure your ESXi hosts to forward syslog data to one or more intermediate Splunk Enterprise forwarders. Use the vSphere Client to enable the syslog firewall for the specific hosts. For vSphere 6.x to 7.0 versions, you don't need to add permissions beyond the default permissions that vSphere provides when creating a role.

Permission
System.Anonymous
System.Read
System.View
Host.Config.AdvancedConfig

Validate vCenter Servers time synchronization settings

Verify time synchronization throughout your environment to improve visibility into application and operating system health. Check the time synchronization for the following components in your environment.

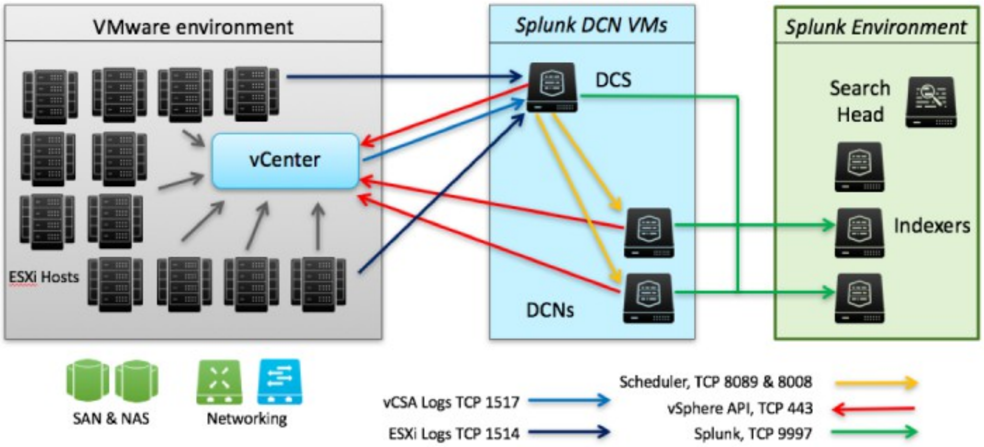
- Hosts
- Splunk Enterprise search head and indexers

Consider using NTP or VMware host/guest time synchronization.

Configure ports

Collect data from vCenter Server systems using the VMware API

The Splunk Add-on for VMware and its prerequisite add-ons use the VMware API to collect data about your virtual environment. The Splunk Add-on for VMware and its prerequisite add-ons communicate with vCenter Server using network ports and Splunk management ports.



This table lists the components that communicate with each other and the ports they use to communicate.

Sender	Receiver	Port number	Description
Collection Configuration	vCenter server	443	Uses port 443 to connect to the vCenter Server to verify that the vCenter Server credentials are valid. It uses this port to discover the number of managed ESXi hosts in the environment.
Splunk Add-on for VMware	Data Collection Node	8089	Connects to the Data Collection Node (DCN) on the default Splunk management port, TCP 8089.

Collection Configuration	Data Collection Node	8008	When the DCN and Splunk Add-on for VMware have established a connection, the Collection Configuration dashboard, which typically runs on the search head, allocates data collection jobs to the DCN on the TCP port 8008 (gateway port). In your environment, if another service uses port 8008, you can configure a different port for communication between the data collection node and the gateway. Data collection nodes do not have to communicate on the same port.
			`[default]`
			`gateway_port = 8008`
			To change the ports for each data collection node individually, set the port in each stanza.

Data Collection Node (DCN)	vCenter Server	443	Communicates with vCenter Server API on port 443 to execute the data collection tasks allocated to it.
Data Collection Node	Splunk indexer	9997	Uses port 9997 to forward data it has retrieved from the vCenter Server using the API.

After the Splunk Add-on for VMware establishes a connection with vCenter Server, the DCN uses port 443 to obtain the credentials for vCenter Server. The DCN uses port 443 to determine the kind of data to collect, such as performance, inventory, or hierarchy data. The Splunk Add-on for VMware sends information to the data collection nodes using port 8008 about the information they need to collect from a specific vCenter Server system. The DCN retrieves the data from vCenter Server and forwards the data to the Splunk indexer on port 9997.

Collect log data from vCenter Server systems and ESXi hosts

You can collect log data from the vCenter Server system and the ESXi hosts in your environment. This table describes how the entities in your environment communicate.

Sender	Receiver	Port number	Description
vCenter server	Splunk indexer	9997	To send log data from the vCenter Server system on port 9997, install the Splunk Universal Forwarder and the Splunk_TA_vcenter on the vCenter Server system. If firewall issues prevent you from installing the Splunk Add-on for vCenter Logs (Splunk_TA_vcenter) components on vCenter Server, forward the vCenter Server log data to the data collection node (DCN). The DCN contains all of the components required to collect vCenter Server log data. Forward this data from the DCN to Splunk indexers.
ESXi host	DCN/ Syslog server	TCP port 1514 / UDP port 514	Prior to ESXi version 6.x, ESXi versions supported either TCP or UDP, but not always both. For an environment with fewer than 40 ESXi hosts, send syslog traffic to the Data Collection Scheduler (DCS), which controls the collection by DCNs. In a larger production environment, use a central syslog server with a Splunk Universal Forwarder and Splunk_TA_esxilogs add-on installed on it. Alternatively, you can send syslog to another DCN virtual machine dedicated to run as a syslog server for the ESXi hosts.
vCenter Servert	DCN/ Syslog server	TCP Port 1517	To send log data from vCenter Linux Server on port 1517 use Syslog-ng/rsyslog. See Collect vCenter Server Appliance logs via syslog.

Prepare to host a data collection node

The Splunk Add-on for VMware uses a virtual appliance version of the Data Collection Node (DCN) to collect performance metrics. Splunk distributes this as an Open Virtual Appliance (OVA) file called the Splunk OVA for VMware metrics.

Splunk configures the DCN with the following default configuration:

- Eight cores. 8 vCPUs or 4 vCPUs with two cores with a reservation of 2GHz.
- 12GB memory with a reservation of 1GB.
- 16GB of disk space.

In production, the DCNs communicate with the Collection Configuration dashboard, which runs on the Splunk search head, to retrieve data from vCenter Server. To ensure reliable communication between systems, use static IP addresses and dedicated host names for each DCN. See Collect Data from vCenter Server systems using the VMware API.

Prepare to deploy the DCN

- Identify the vCenter servers and managed ESXi hosts from which you want to collect data.
- Determine the number of DCNs that you want to deploy. Each DCN can collect data from 70 or fewer ESXi hosts, based on the specifications for the 8 core DCN configured with the OVA for VMware with a ratio of 25 to 30 virtual machines per host.
- Each Data Collection Node (DCN) needs at least one CPU core for every 10 hosts from which the DCN is collecting data.
- Estimate the number of CPUs needed for your worker processes with the expectation that a CPU in your deployment can be kept as a spare for other processes. Provision at least one extra CPU to help promote capacity and availability in your deployment.
- Obtain static IP addresses and host names to apply to each of the DCNs.

Identify if a dedicated Distributed Collection Scheduler is needed

A Linux-based dedicated Distributed Collection Scheduler (DCS) is required if any of the following scenarios apply.

- Your search head is running on Windows
- Your search heads are in a search head cluster
- Site-specific collection is desired

If one or more of the cases above is true, you must plan to have an additional Splunk instance running on Linux to perform the collection. (The OVA image above can be used to create this additional instance.)

When you have this information, you can then create the data collection nodes. For more information, see Configure the Splunk OVA for VMware Metrics.

Install the Splunk Add-on for VMware in an on-premises environment

The Splunk Add-on for VMware performs several data collection and enrichment tasks. This guide takes you through installing the Splunk Add-on for VMware and its prerequisite add-ons in preparation for configuring data collection.

1. Upload the Splunk_TA_vmware and SA-Hydra packages from Splunk Add-on for VMware to the data collection nodes.

2. Upload the Splunk_TA_vmware and SA-Hydra packages from Splunk Add-on for VMware to the data collection scheduler.
3. Upload the packages from the in Splunk Add-on for VMware Indexes, Splunk Add-on for vCenter Logs, Splunk Add-on for VMware ESXi Logs add-ons to the indexer(s).
4. Add the packages from the Splunk Add-on for vCenter Logs, Splunk Add-on for VMware ESXi Logs, and Splunk Add-on for VMware Extractions to the search head(s).
5. Add add-on components to forwarders (for log collection).
6. Create a distributed collection scheduler. Data collection for VMware requires complex job management for connecting to and polling data from your environment. The scheduler is a Splunk component used to manage data collection jobs between your data collection nodes.

This table outlines a distributed deployment installation of the Splunk Add-on for VMware and its prerequisite add-ons. For single deployments, all components have to be installed on your single Splunk platform instance. The Splunk Add-on for VMware can't be installed using Splunk Web.

Splunkbase Add-on	Component	Search head	Scheduler (DCS)	Indexer	Data Collection Node (DCN)	Dedicated ESXi log forwarder	Dedicated vCenter log forwarder
Splunk Add-on for VMware	Splunk_TA_vmware SA-Hydra		X		X		
Splunk Add-on for ESXi Logs	Splunk_TA_esxilogs	X		X		X	
Splunk Add-on for vCenter Logs	Splunk_TA_vcenter	X		X	Optional*		X
Splunk Add-on for VMware Indexes	SA-VMWIndex			X			
Splunk Add-on for VMware Extractions	TA-VMW-FieldExtractions	X					

(*)Depending on your specific configuration, you might also need Splunk_TA_vcenter to collect VCenter data.

Forwarding vCenter application logs to Syslog, an intermediate forwarder, or directly to a Splunk indexer is supported from 6.x to 7.0 versions of vCenter Server.

Upload the Splunk Add-on for VMware to your Data Collection Nodes

If this is an upgrade from a previous version of The Splunk Add-on for VMware or the Splunk App for VMware, follow the steps below. Otherwise, you will need to configure data collection nodes to connect to and poll data from your VMware vCenters. Steps for setting up a Data Collection node can be found here

1. Stop your Splunk platform instance on each of your DCNs.
2. Upload Splunk_TA_vmware and SA-Hydra to each of your DCNs.
3. Restart your Splunk platform instance each of your DCNs.

Upload the prerequisite add-on for Splunk Add-on for VMware to your search heads

> If you are installing the Splunk Add-on for VMware on a search head cluster in a distributed deployment, you have to use a dedicated scheduler. To deploy the add-ons listed below, follow the guidance in Install an add-on in a distributed Splunk Enterprise deployment.

1. Stop your Splunk platform instance.
    1. If you are using a search head cluster, extract the packages Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs), Splunk Add-on for vCenter Logs (Splunk_TA_vcenter), and Splunk Add-on for VMware Extractions (TA-VMW-FieldExtractions) from Splunkbase to $SPLUNK_HOME/etc/shcluster/apps/ on the deployer.
    2. If you are not using a search head cluster, extract and upload the Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs), Splunk Add-on for vCenter Logs (Splunk_TA_vcenter), and Splunk Add-on for VMware Extractions (TA-VMW-FieldExtractions) packages from Splunkbase to $SPLUNK_HOME/etc/apps.

        > Note: No packages from Splunk Add-on for VMware are required on the search head.
2. Restart your Splunk platform instance.

> Note: The Hydra troubleshooting dashboards are now part of the Splunk Add-on for VMware Extractions. So, the SA-Hydra package isn't required on the search head for v4.0.3.

Update the default character count limitations for the search commands

The Splunk Add-on for VMware collects the VMware infrastructure inventory data. Because inventory data can have a much higher length for the collected JSON data, it might exceed the default length limit of 5000 characters. Complete the following steps to change the character length limit:

For search head cluster deployments

1. Create a new file with the name limits.conf in the `$SPLUNK_HOME/etc/shcluster/apps/TA-VMW-FieldExtractions/local` directory on the deployer.
2. Add the following stanza to the limits.conf file:

    ```
    [spath]
    # number of characters to read from an XML or JSON event when auto extracting
    extraction_cutoff = 20000
    extract_all = true
    ```
3. Push the app bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer does not restart the search head cluster members, perform a rolling restart.

For dedicated search head deployments

1. Create a new file with the name limits.conf in the `$SPLUNK_HOME/etc/apps/TA-VMW-FieldExtractions/local` directory on the search head.
2. Add the following stanza to the limits.conf file:

    ```
    [spath]
    ```

```
# number of characters to read from an XML or JSON event when auto extracting
extraction_cutoff = 20000
extract_all = true
```

3. Restart the Splunk instance.

Upload the prerequisite add-on for Splunk Add-on for VMware to your indexer cluster deployment

1. Enable maintenance mode on indexer master node.
2. Download and extract the components of the Splunk Add-on for VMware Indexes (SA-VMWIndex), the Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs), and the Splunk Add-on for vCenter Logs (Splunk_TA_vcenter) to etc/master-apps on indexer master node.
3. Restart indexer master node.
4. Push configuration bundle from indexer master node.

Upload the prerequisite add-on for the Splunk Add-on for VMware to non-clustered indexer(s)

1. Stop your Splunk indexer instance.
2. Download and extract the components of the Splunk Add-on for VMware Indexes (SA-VMWIndex), the Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs), and the Splunk Add-on for vCenter Logs (Splunk_TA_vcenter) to etc/apps.
3. Restart your Splunk indexer instance.

Upload the prerequisite add-on for the Splunk Add-on for VMware to forwarders

Collect logs from VMware vCenter and ESXi hosts by sending them through an intermediate forwarder or directly to your Splunk indexers.

> Skip this step if you are forwarding logs directly to Splunk indexers from your ESXi hosts and vCenter Servers.

1. Stop the forwarder
2. On forwarder, under splunkforwarder/etc/apps, upgrade Splunk Add-on for VMware ESXi Logs(Splunk_TA_esxilogs) and Splunk Add-on for vCenter Logs(Splunk_TA_vcenter).
3. The new add-on package includes props.conf and inputs.conf changes for vclogs, so user must update `/local` directory with these two files and enable the appropriate stanzas.
4. Make sure under etc/system/local/output.conf, server entries to forward logs to your indexer(s) are present.
5. Restart the forwarder

Upload Splunk Add-on for VMware to your scheduler

The scheduler is the instance of Splunk that manages connections to the Data Collection Nodes and manages data collection jobs across your DCNs and vCenters. For production environments the scheduler should not be on the same search head as your VMware App. We recommend using a license server, distributed management console or a stand alone Splunk instance as your scheduler.

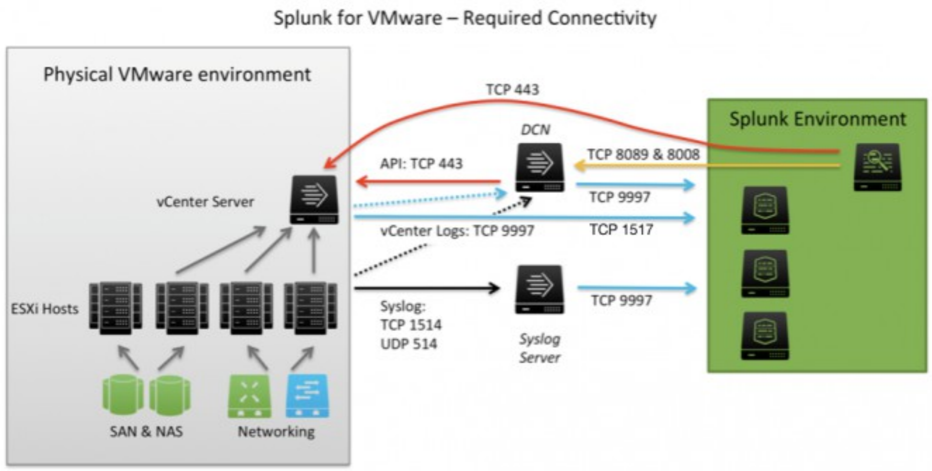
1. Stop Scheduler.
2. Collection configuration UI is now present in TA VMware: upload **Splunk_TA_vmware** and **SA-Hydra** to `etc/apps`.
3. Start the scheduler.

Configure the Splunk Add-on for VMware to collect data

Configure the Splunk Add-on for VMWare to collect Data Collection Node and Virtual Center data. Identify the data types that you want to collect, such as performance, inventory, or hierarchy data, from the following list.

- vCenter logs (Intermediate Forwarder/Syslog Forwarder)
- ESXi logs (Intermediate Forwarder/Syslog Forwarder)
- Performance Metrics, Inventory, Tasks (vCenter API collected by Data Collection Node)

This table lists the components that communicate with each other and the ports they use to communicate.



Configure collection of Performance, configuration, and event data

Validate time synchronization

Verify time synchronization throughout your environment to improve visibility into application and operating system health. Check the time synchronization for the following components in your environment.

- Hosts
- Splunk Enterprise search head and indexers

Consider using NTP or VMware host/guest time synchronization.

Configure the Splunk Add-on for VMware to collect data from vCenter logs

vCenter logs contain information about access to the vCenter environment, audit information (who assigned permissions, added/edited/removed VMs), and health information about vCenter's processes.

For vCSA servers, vCSA's native syslog forwarding is used to pass this information to your Splunk platform. Nothing is installed onto the vCSA servers to collect this data. Windows-based vCenter environments require a Splunk platform forwarder and Splunk Add-on for vCenter Logs(Splunk_TA_vcenter).

Prepare to collect data

Set up a vCenter Server user account

Obtain VMware vCenter Server account credentials for each vCenter Server system.

These credentials allow the Splunk Add-on for VMware read-only API access to the appropriate metrics on each vCenter Server system in the environment. the Splunk App for VMware uses the credentials when the DCN polls vCenter Server systems for performance, hierarchy, inventory, task, and event data. These credentials are required for DCN configuration. You can use existing vCenter Server account credentials, or create a new account for Splunk App for VMware to access the vCenter Server data.

If you encounter issues setting the correct permissions for vCenter Server accounts, see "Permissions in vSphere."

You must have a user account to authenticate with vCenter. Your role determines access privileges. If you use ActiveDirectory for authentication on your Windows OS (vCenter) machines, see *Create users in ActiveDirectory* in this topic.

If you add a new vCenter Server user as administrator, the user automatically gets an Administrator role in vSphere.

Create a local user on your Windows OS (vCenter) machine

1. Log into the Windows OS with an administrator account.
2. In the **Start** menu, click **Control Panel**.
3. In the User Accounts screen, click **Add or remove user accounts**.
4. In the Manage Accounts window, click **Create a new account.**
5. Enter a name for the account (example: **splunksvc**).
6. In vSphere, select **Standard user**.
7. Click **Create Account**.

8. In the Manage Accounts screen, click on the new user.
9. In the Change an Account screen, click **Create a password** and assign the user a password. The new user account displays as a **Standard user** and the account shows that it is **Password protected**.
10. Verify that you now have a local Windows user compatible with the vSphere permissions system.

Create users in Active Directory

For machines that participate in an Active Directory (AD) domain, create a service account in the given domain using the appropriate control panel in Windows Server. Most VMware environments use a single Active Directory domain for authentication. However, if you use multiple AD domains, then create a service account in each domain that your VMware environment uses.

How you create a service account within Active Directory depends on your environment. Contact your AD administrator to learn how to do this for your environment.

Create roles on each vCenter server in your environment

1. Open the vSphere client and connect to the vCenter server.
2. Log in with administrative privileges.
3. Click **Home** in the path bar.
4. Under **Administration** click **Roles**.
5. Click **Add Role**.
6. In the **Add new Role** dialog box, enter a name for the role (for example, splunkreader).
7. Select the appropriate permissions for the role.

For information about collecting data via the VMware API, see Configure the Splunk Add-on for VMware to collect data from vCenter Server systems using the VMware API.

Configure DCNs to honor TLS protocols

You may need to set your DCN's to honor TLS protocols when making requests to the vCenter APIs.

1. On your DCN, Navigate to $SPLUNK_HOME/etc/system/local, and open `web.conf` with a text editor. If there is no web.conf create the file.
2. Add the below stanzas to your `web.conf` file.

```
[settings]
sslVersions = tls1.2
cipherSuite = AES256-SHA256
```

Validate and patch vCenter Server systems, add WSDL files

If you use vCenter Server 5.0 and 5.0.1, apply a patch to manage a known issue with the servers. See known issues in the release notes for details on acquiring and applying the patch.

If you use vSphere 5.0 or 5.0 update 1, be sure to add two missing WSDL files that the app needs to make API calls to vCenter. Access the VMware Knowledge Base for detailed installation instructions. The missing files are:

- `reflect-message.xsd`
- `reflect-types.xsd`

vCenter Log Collection (Windows vCenter and vCSA)

Collect Windows VMware vCenter Server log data

Use the Splunk Add-on for VMware vCenter to collect vCenter Server log data. Use a Splunk Universal Forwarder to forward the log data from your Windows vCenter Server to the indexer.

1. Install a Splunk forwarder.

    - Download the Universal Forwarder.
    - Install the Universal Forwarder. See Install a Universal Forwarder on Windows.

- Configure forwarding. Configure the forwarder on your vCenter Server systems to send data to your indexers. Configure the forwarder in the `outputs.conf` file for each forwarder installed on a vCenter Server system. See Configure forwarding with outputs.conf.
- Change your Splunk password.

    - The default password for the Splunk Enterprise admin user is `changeme`. Change the password using Splunk Web. See "Change the admin default password" in the *Admin Manual*.

- Install the Splunk Add-on for vCenter Logs (Splunk_TA_vcenter).

    - Get the file `Splunk_TA_vcenter-<version>-<build_number>.zip` from the download package and install it on your vCenter Server systems.
    - Unzip the file, `"Splunk_TA_vcenter-<version>-<build_number>.zip"`, into the `apps` directory under `%SPLUNK_HOME%\etc\apps`. When installing on a universal forwarder the path is `C:\Program Files\SplunkUniversalForwarder\etc\apps` otherwise it is `C:\Program Files\Splunk\etc\apps`.

- On the system where you've installed the Splunk Enterprise forwarder, install the Splunk Add-on for vCenter Logs (Splunk_TA_vcenter).
- Copy the inputs.conf file from `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default`.
- Paste `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default` into the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/local` folder.
- Open the inputs.conf file.
- Change the log path to the location of the vCenter Server Appliance logs data, `C:\ProgramData\VMware\vCenterServer\logs`. Edit the following stanzas in the inputs.conf file:

Windows vCenter server 6.x

```
[monitor://$ALLUSERSPROFILE\VMware\vCenterServer\logs\vws]
disabled = 0
index = vmware-vclog

[monitor://$ALLUSERSPROFILE\VMware\vCenterServer\logs\vmware-vpx]
blacklist = (.*(gz)$)|(\\drmdump\\.*)
disabled = 0
index = vmware-vclog

[monitor://$ALLUSERSPROFILE\VMware\vCenterServer\logs\perfcharts]
disabled = 0
index = vmware-vclog
```

- (Optional) If you configured Splunk Enterprise as a heavy or light forwarder, and you want to monitor the license file and and tomcat configuration files, edit the following stanzas in the props.conf file.

- Copy the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default/props.conf` file.
- Paste `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default/props.conf` into the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/local` folder.
- Open the local props.conf file.
- Change the log path to that in which the vCenter Server Appliance logs data. Adjust the following stanzas:

Windows vCenter server

```
[source::(?-i)...\\VMware\\vCenterServer\\logs\\cim-diag.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\sms.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\stats.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\vim-tomcat-shared.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\vpxd-\d+.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\vpxd-alert-\d+.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\vpxd-profiler-\d+.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\vws.log(?:.\d+)?]
[source::(?-i)...\\VMware\\vCenterServer\\logs\\vpxd.cfg]
```

- Change the licenses path to the vCenter Server Appliance licenses path:

```
[source::(?-i)...\\VMware\\vCenterServer\\licenses]
```

- Change the tomcat conf path to the vCenter Server Appliance tomcat conf path:

```
[source::(?-i)...\\VMware\\Infrastructure\\tomcat\\conf]
```

- Change the path to the vCenter Server Appliance path:

```
[source::...\\Application Data\\VMware\\â ¦]
[source::...\\VMware\\Infrastructure\\â ¦]
```

- Restart Splunk Enterprise. See "Start and stop Splunk" in the *Admin Manual*.
- In `%SPLUNK_HOME%\bin` run the command `splunk restart`. Alternatively, select **Start** > **Administrative Tools** > **Services** > Splunkd restart in **Windows services**.

The Splunk Add-on for VMware collects log data from your Windows vCenter Server systems and forwards the data from vCenter Server to your Splunk platform indexers or combined indexer search heads.

Collect VMware vCenter Server Appliance (vCSA) log data

Use the Splunk Add-on for VMware to collect logs from the VMware vCenter Server Appliance. the Splunk Add-on for VMware stores VMware vCenter Server Appliance logs in `/var/log/vmware`.

- Export vCenter logs to another system on which you have installed Splunk Enterprise.
- Install a Splunk Enterprise forwarder on the same machine to forward the VMware vCenter Linux appliance logs. See "Forward VMware vCenter Linux appliance logs to Splunk Enterprise".

Export vCenter logs to an external system

1. Install a Splunk forwarder.

- Download the Universal Forwarder.

    - Install the Universal Forwarder. See Install Universal Forwarder on *nix in the Splunk **Universal Forwarder Manual**.

- Enable the VMware vCenter Server Appliance to store log files on NFS storage on a system on which you have installed Splunk Enterprise as a **heavy forwarder** or as a **light forwarder**. See NFS Storage on the VMware vCenter Server Appliance in the VMware vSphere documentation.
- On the system on which you have installed the Splunk Enterprise forwarder, install the Splunk Add-on for vCenter Logs (Splunk_TA_vcenter).
- Copy the `inputs.conf` file from `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default` then paste it into the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/local` folder and open file.
- Change the log path to the location that the vCenter Server Appliance logs data (`/var/log/vmware/`). Edit the following stanzas in the `inputs.conf` file: Linux server appliance 6.x, 7.0.

```
[monitor:///var/log/vmware/vws]
disabled = 0
index = vmware-vclog

[monitor:///var/log/vmware/vpxd]
blacklist = (.*(gz)$)|(\\drmdump\\.*)
disabled = 0
index = vmware-vclog

[monitor:///var/log/vmware/perfcharts]
disabled = 0
index = vmware-vclog
```

  Linux server appliance 6.x, 7.0 (not supported from 3.4.5)

```
[monitor:///var/log/vmware/vpx]
blacklist = (.*(gz)$)|(\\drmdump\\.*)
disabled = 0
index = vmware-vclog
```

- (Optional) If you configured Splunk Enterprise as a heavy/light forwarder and you want to monitor the license file and tomcat configuration files, edit the following stanzas in the props.conf file:

    - Copy the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default/props.conf` file, then past into the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/local` folder. Open the local `props.conf` file.

    - Change the log path to that in which the vCenter Server Appliance logs data. Adjust the following stanzas:

  Linux server appliance 6.x

```
[source::(?-i).../var/log/vmware/perfcharts/stats.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpxd/vpxd-\d+.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpxd/vpxd-alert-\d+.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpxd/vpxd-profiler-\d+.log(?:.\d+)?]
```

  Linux server appliance 5.x (not supported from 3.4.5)

```
[source::(?-i).../var/log/vmware/vpx/stats.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpx/vpxd-\d+.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpx/vpxd-alert-\d+.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpx/vpxd-profiler-\d+.log(?:.\d+)?]
[source::(?-i).../var/log/vmware/vpx/vws.log(?:.\d+)?]
```

- Start Splunk Enterprise.

Forward VMware vCenter Linux appliance logs to Splunk Enterprise

To forward VMware vCenter Linux appliance logs to your Splunk Enterprise indexers or search head, install a Splunk Enterprise forwarder on the VMware vCenter Linux appliance. Access to vCSA shell access must be enabled.

1. Install a Splunk forwarder on the VMware vCenter Server Appliance.
2. Download the Splunk Add-on for vCenter Logs (Splunk_TA_vCenter) from Splunkbase and extract its contents to the $SPLUNK_HOME/etc/apps directory.
3. Copy the `inputs.conf` file from `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default` then paste it into the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/local` folder and open file.
4. (Optional) If you configured Splunk Enterprise as a **heavy forwarder** and you want to monitor the license file and and tomcat configuration files, copy the contents of the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default/props.conf` file and paste it into the `$SPLUNK_HOME/etc/Splunk_TA_vCenter/local` folder.
5. Start the Splunk Universal Forwarder.

Collect vCenter Server Appliance logs via syslog

Syslog type	Supported vCSA version	Log types
syslog-ng	5.5	`vpxd`, `vpxd-profiler`, `vpxd-alert`
rsyslog	6.x, 7.0	`vpxd`, `vpxd-profiler`, `vpxd-alert`

Syslog-ng on vCenter 5.5

> vCenter 5.5 is not supported from VMware 3.4.5

Enable syslog forwarding using syslog-ng for vCSA 5.5 logs.

1. Open your vCenter deployment, and navigate to `/etc/syslog-ng/`.
2. In `/etc/syslog-ng/`, open the `syslog-ng.conf` file.
3. In the `syslog-ng.conf` file, replace `<IP/HOSTNAME>` with the IP address of the hostname of the machine where you want to receive the vCSA logs.

   Example:

```
# vpxd source log
source vclog {
    file("/var/log/vmware/vpx/vpxd.log" follow-freq(60) log-prefix("vpxd ") flags(no-parse));
    file("/var/log/vmware/vpx/vpxd-alert.log" follow-freq(60) log-prefix("vpxd-alert ")
flags(no-parse));
    file("/var/log/vmware/vpx/vpxd-profiler.log" follow-freq(60) log-prefix("vpxd-profiler ")
flags(no-parse));
    file("/var/log/vmware/vpx/vws.log" follow-freq(60) log-prefix("vws ") flags(no-parse));
    file("/var/log/vmware/vpx/stats.log" follow-freq(60) log-prefix("stats ") flags(no-parse));
    file("/var/log/vmware/vpx/cim-diag.log" follow-freq(60) log-prefix("cim-diag ")
flags(no-parse));
    file("/var/log/vmware/vpx/sms.log" follow-freq(60) log-prefix("sms ") flags(no-parse));
    file("/var/log/vmware/vpx/cim-diag.log" follow-freq(60) log-prefix("cim-diag ")
flags(no-parse));
    file("/var/log/vmware/vpx/vmware-vpxd.log" follow-freq(60) log-prefix("vmware-vpxd ")
flags(no-parse));
};

# Remote Syslog Host
destination remote_syslog {
    tcp("<IP/HOSTNAME>" port(1517) template("${MSG} \n") template-escape(no));
};

# Log vCenter Server vpxd log remotely
log {
            source(vclog);
            destination(remote_syslog);
};
```

4. After changing the conf file, restart the syslog service for the changes to take effect. `service syslog restart`
5. Navigate to `Splunk/etc/apps/Splunk_TA_vcenter/` and create a local folder.
6. In `Splunk/etc/apps/Splunk_TA_vcenter/local`, create an inputs.conf file.
7. Navigate to `Splunk/etc/apps/Splunk_TA_vcenter/default/inputs.conf` and copy the below stanza.

```
#[tcp://1517]
#connection_host = dns
#index = vmware-vclog
#sourcetype = vclog
#disabled = 0
```

8. Navigate to `Splunk/etc/apps/Splunk_TA_vcenter/local/inputs.conf`, and paste the copied stanza into the local version of `inputs.conf`.
9. Enable the copied stanza in `local/inputs.conf` by uncommenting it.

   Note: Since TCP port 1514 is used for receiving ESXi logs, the 1517 port is used, by default, for vclogs. Other open ports can be used.

File properties	Description
`follow-freq`	Used to set the polling interval in seconds.
`log-prefix`	Used to set the prefix in each event data. Set log-prefix so your Splunk platform deployment can recognize sourcetype of different logs.
`flags`	Used to forward the log without any parsing.

For more information on configuration details, see the syslog-ng Open Source Edition Administrator Guide

Rsyslog on vCenter 6.x, 7.0

Enable syslog forwarding using rsyslog for vCSA 6.x or 7.0 logs.

1. Open your vCenter deployment, and navigate to `/etc/`.
2. In `/etc/`, open the `rsyslog.conf` file.
3. In the `rsyslog.conf` file, replace `<IP/HOSTNAME>` with the IP address of the hostname of the machine where you want to receive the vCSA logs.

   Example:

```
$template vclogtemplate,"%syslogtag% %rawmsg%"

$ModLoad imfile
```

```
$InputFileName /var/log/vmware/vpxd/vpxd.log
$InputFileTag vpxd
$InputFileStateFile state-vpxd
$InputFileSeverity all
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /var/log/vmware/vpxd/vpxd-profiler.log
$InputFileTag vpxd-profiler
$InputFileStateFile state-vpxd-profiler
$InputFileSeverity all
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /var/log/vmware/vpxd/vpxd-alert.log
$InputFileTag vpxd-alert
$InputFileStateFile state-vpxd-alert
$InputFileSeverity all
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /var/log/vmware/vws/watchdog-vws/watchdog-vws-syslog.log
$InputFileTag vws
$InputFileStateFile state-vws
$InputFileSeverity all
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /var/log/vmware/perfcharts/stats.log
$InputFileTag stats
$InputFileStateFile state-stats
$InputFileSeverity all
$InputRunFileMonitor

 *.* @@<IP/HOSTNAME>:1517;vclogtemplate
```

4. After changing the conf file, restart the syslog service for the changes to take effect. `service syslog restart`
5. Navigate to `Splunk/etc/apps/Splunk_TA_vcenter/` and create a local folder.
6. In `Splunk/etc/apps/Splunk_TA_vcenter/local`, create an inputs.conf file.
7. Navigate to `Splunk/etc/apps/Splunk_TA_vcenter/default/inputs.conf` and copy the below stanza.

```
#[tcp://1517]
#connection_host = dns
#index = vmware-vclog
#sourcetype = vclog
#disabled = 0
```

8. Navigate to `Splunk/etc/apps/Splunk_TA_vcenter/local/inputs.conf`, and paste the copied stanza into the local version of `inputs.conf`.
9. Enable the copied stanza in `local/inputs.conf` by uncommenting it.

   Note: Since TCP port 1514 is used for receiving ESXi logs, the 1517 port is used, by default, for vclogs. Other open ports can be used.

File properties	Description
`$InputFileName`	Used to monitor specific files.
`$InputFileTag`	Used to set the prefix in each event data. Set `$InputFileTag` so your Splunk platform deployment can recognize sourcetype of different logs.

File properties	Description
`$InputFileStateFile`	Used to keep track of which parts of the monitored file are already processed. Must be unique.
`$InputFileSeverity`	Used to set the type of log the user wants.
`$InputRunFileMonitor`	Used to activate the monitoring.

For more information on configuration details, see the text file input module page.

Configure the Splunk Add-on for VMware to collect log data from ESXi hosts

ESXi server logs let you troubleshoot events and host issues.

Splunk Add-on for VMware accepts ESXi log data using syslogs from the following sources.

- A Splunk platform forwarder as the data collection point, which can be the Splunk OVA for VMware. When you use the forwarder to collect ESXi logs, Splunk platform is the default log repository.
- A syslog server with a Splunk platform forwarder monitoring logs.

The VMware environment supports the following ports for syslog data collection.

- TCP port 1514: Not supported on VMware vSphere 4.1.
- UDP port 514: Requires Splunk Enterprise root privileges.

Configure the Splunk Add-on for VMware ESXi logs to receive ESXi syslog data

- To configure ESXi log data collection, identify the machine to use as your data collection point. Verify that the ESXi hosts can forward data to that data collection point.
- For the first installation, use an intermediate forwarder as your data collection point. Configure hosts to forward syslog data to the intermediate forwarder.

Step 1: Install a Splunk Universal Forwarder on your syslog server

1. Download the Splunk Universal Forwarder from Download Splunk Universal Forwarder page. Select the forwarder version and the OS version that you need.
2. See "Deployment overview" in *Forwarding Data* to install the universal forwarder.

Step 2: Create an inputs.conf file

Create an `inputs.conf` file in the `system/local` folder to monitor the ESXi hosts log files on the syslog server. Set the index and the source type before sending it to the intermediate forwarder.

1. For each monitor stanza in the `inputs.conf` file, specify the following settings:
    - sourcetype: `vmw-syslog`
    - index: `vmware-esxilog`. See "Configure your inputs" in *Getting Data In* for more information.

   The entry in the monitor stanza of the `inputs.conf` file is:

   ```
   [monitor:///var/log/.../syslog.log]
   disabled = false
   index = vmware-esxilog
   sourcetype = vmw-syslog
   ```

2. Configure forwarding on your syslog server in `outputs.conf` to send data to your indexer or intermediate forwarder, which is the Splunk Enterprise instance on which Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs) is installed. For more information about setting up forwarding for your indexers, see Configure forwarders with outputs.conf in *Forwarding Data*.

Step 3: Install and configure Splunk_TA_esxilogs

Install and configure Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs) on the machine that receives log data from your syslog server.

Install Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs) under $SPLUNK_HOME/etc/apps. This technology add-on is included in Splunk App for VMware. It collects syslog data from the ESXi hosts and maps the data into the dashboards in Splunk App for VMware.

Step 4: Configure Splunk Add-on for VMware ESXi Logs

1. Assign the `host` field (on the machine where Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs) is installed). The Splunk Add-on for VMware can not determine the originating host for the data when you use a syslog server as your data store and you forward that data to the Splunk platform indexer.
2. (Optional) Create an index time extraction that takes the actual host name from the event that passes through, so that the log files can be associated with the correct host. By default, the host name is that of the syslog server. This step is not required when you use an intermediate forwarder, as the Splunk App for VMware automatically assigns the host based on the original data source.
3. Assign the `host` field. Create a local version of `props.conf` and `transforms.conf` in the `$SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/local/` directory and add the regular expressions to extract the host field. In this example regular expression extraction in `props.conf` calls the `set_host` stanza of `transforms.conf` where the regular expression extraction extracts the host. The source and sourcetype fields are extracted by the settings in the `props.conf` and `transforms.conf` files in `$SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/default`. Do not override these fields in the local versions of these files. Example of the entry for props.conf:

   ```
   [vmw-syslog]
   â ¦â ¦
   TRANSFORMS-vmsysloghost = set_host
   ```

   Here's the example for `transforms.conf`

   ```
   [set_host]
   REGEX = ^(?:\w{3}\s+\d+\s+[\d\:]{8}\s+([^ ]+)\s+)
   DEST_KEY = MetaData:Host
   FORMAT = host::$1
   ```
4. If the sourcetype is not correct, check the regular expressions in the stanzas `[set_syslog_sourcetype]` and `[set_syslog_sourcetype_4x]` in `Splunk_TA_esxilogs/default/transforms.conf`.
   The following is an example of an entry in `transforms.conf`:

   ```
   [set_syslog_sourcetype]
   REGEX = ^(?:(?:\w{3}\s+\d+\s+[\d\:]{8})|(?:<\d+>)?(?:(?:(?:[\d\-]{10}T[\d\:]{8}(?:\.\d+)?(?:Z|[\+\
   -][\d\:]{3,5})?))|(?:NoneZ)?)|(?:\w{3}\s+\w{3}\s+\d+\s+[\d\:]{8}\s+\d{4}))\s[^
   ]+\s+([A-Za-z\-]+)(?:[^:]*)[:\[]
   DEST_KEY = MetaData:Sourcetype
   FORMAT = sourcetype::vmware:esxlog:$1
   ```

   Where:

   - `^(?:(?:\w{3}\s+\d+\s+[\d\:]{8})|(?:<\d+>)?(?:(?:(?:[\d\-]{10}T[\d\:]{8}(?:\.\d+)?(?:Z|[\+\-][\d\:]{3,5})?))|(?:NoneZ)?)|(?:\w{3}\s+\w{3}\s+\d+\s+[\d\:]{8}\s+\d{4}))\s[^ ]+\s+` is used to extract the datetime field and host field

- ♦ `([A-Za-z\-]+)` is used to extract the sourcetype
- ♦ `(?:[^:]*)[:\[]` defines the limit. sourcetype is followed by `:` or `[`

Troubleshoot Splunk Add-on for VMware ESXi Logs

- If the time is not extracted from the events, for example, `Mar 26 19:00:20 esx1.abc.com Hostd:â ¦`, you can modify `$SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/default/syslog_datetime.xml` or you can use splunk `datetime.xml` and change the entry for `DATETIME_CONFIG` to `/etc/datetime.xml` in `/local/props.conf`.

- If you use VMware vSphere ESX 4.x, remove the comment tags from the following stanzas in `transforms.conf` on the search head. This ensures that datetime extraction is the same in all regular expressions. These stanzas are only used during search time extraction.

```
[esx_hostd_fields_4x]
[esx_vmkernel_fields_4x]
[esx_generic_fields_4x]
```

- If the correct fields do not display in the ESXi Log Browser, modify the regular expressions in the `[esx_vmkernel_fields]`, and , `[esx_generic_fields]`, stanzas.

The following example is from `transforms.conf`.

```
[esx_vmkernel_fields]
REGEX = (?:^<(\d+)>)?<REPLACE WITH REGEX FOR DATE TIME AND HOST FIELD
EXTRACTION>:(vmkernel|vmkwarning):\s+(?:([\d\:\.]+)\s+)?(cpu\d+):(?:(\d+)\))?(?:\[([\:\w]+)\]\s+)?(.*)
FORMAT = Pri::$1 Type::$2 HostUpTime::$3 Cpu::$4 WorldId::$5 SubComp::$6 Message::$7
[esx_generic_fields]
REGEX = (?:^<(\d+)>)?<REPLACE WITH REGEX FOR SOURCETYPE EXTRACTION>:?\s*(.*)$
FORMAT = Pri::$1 Application::$2 Message::$3
```

Use an intermediate forwarder to configure Splunk to receive syslog data

Step 1: Set up your forwarder

1. Install Splunk Enterprise 6.0.x configured as a heavy forwarder or light forwarder on a machine identified as the intermediate forwarder. If Splunk Enterprise is installed as the heavy forwarder, index time extraction happens on this intermediate forwarder. This forwarder can be the data collection node OVA. We recommend a ratio of one intermediate forwarder to 100 ESXi hosts.
2. Set up forwarding to the port on which the Splunk indexers are configured to receive data. See "Set up forwarding" in *Distributed Deployment*.
3. Download the Splunk Add-on for VMware ESXi Logs from Splunkbase and extract its contents to the SPLUNK_HOME/etc/apps/ directory. Use UDP port 514. As the Splunk user on the intermediate forwarder, you have to have root privileges to configure data inputs. If you don't have the required privileges, use TCP port 1514.

Step 2: Enable the ports to receive syslog data

Enable ports in Splunk Web using **Settings** or by modifying the `inputs.conf` file. In this example using Splunk Web, the TCP port is 1514.

1. Select **Settings > Data Inputs**.
2. Add TCP port 1514.
3. In the **Setup screen** enter the following information:

- ♦ **TCP port**: `1514`
- ♦ **Accept conditions from all hosts**: `yes`
- ♦ **Set sourcetype**: `Manual`
- ♦ **Source type**: `vmw-syslog`

4. Select **More Settings** and enter the following information:
   - ♦ **Set host**: `DNS`
   - ♦ **Set the destination index for the source**: **vmware-esxilog**. This setting is the destination of the syslog data. Set the destination index for the source after you have installed the Splunk App for VMware components.

If you do not have access to Splunk Web, create an inputs.conf file in `$SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/local/` and copy the following stanza from `$SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/default/inputs.conf`:

```
#[tcp://1514]
#index = vmware-esxilog
#sourcetype = vmw-syslog
#connection_host = dns
#disabled = 0
```

Uncomment the above stanza in the inputs.conf of local folder.

Note: Do the same for UDP stanza if you are sending data to UDP port(514).

Configure ESXi hosts to send data

Configure the ESXi hosts to forward log data to your syslog server or intermediate forwarders. Enable syslog data collection on the firewall on each host from which you want to collect syslog data.

Configure ESXi hosts using the vSphere Client

1. Select a host on the Hierarchy selector.
2. Click the **Configuration** tab.
3. In the Software section, click **Advanced Settings**.
4. In Advanced Settings, scroll down and select Syslog.
5. Change the setting `Syslog.global.loghost` to the machine receiving the data. For example, enter `tcp://yourmachine.yourdomain:1514`. To forward the logs to multiple destinations, place , between the two machine specifications. For example, enter `tcp://yourmachine1.yourdomain:1514, tcp://yourmachine2.yourdomain:1514`. vSphere version 4.1 forwards only to tcp. In this case, do not specify `tcp://`. ESXi hosts forward to UDP port 514 or TCP port 1514 by default. To forward to UDP port 514, make sure that the receiving machine is set up to do so. To forward to a different port, create a new outbound firewall rule as another Security Profile on the sending host.
6. Click **OK**.
7. In Software, click **Security Profile**.
8. In Firewall, click **Properties**.
9. In Firewall Properties Remote Access, select **Syslog**.
10. Click **Firewall**.
11. Select **Allow connections from any IP address** or specify the connections.
12. Click **OK**.

Set up a host profile

The VMware ESXi and vCenter Server documentation describes how to set up syslog from a host profile.

- See Set Up Syslog from the Host Profiles Interface in the VMware ESXi and vCenter Server 5 Documentation.
- See Set Up Syslog from the Host Profiles Interface in the vSphere Client 5.1.

Configure all hosts remotely

Splunk App for VMware can configure hosts remotely when you use an intermediate forwarder to collect syslog data. See **Configure data collection.**

Configure the Splunk Add-on for VMware to collect log data from vCenter Server systems using the VMware API

The Splunk Add-on for VMware uses the VMware API to collect data about your virtual environment. VMware add-on collects Inventory data at default interval defined in `Splunk_TA_vmware\default\ta_vmware_collection.conf` configuration file. Since it is not needed to collect full inventory data at every interval, the add-on is designed to collect full inventory data in collectionVersion 1 and then it will collect only change sets (e.g. changes in VM inventory or host inventory) in incremental collectionVersions. After 4 hours or collectionVersion 20, whichever is earlier, add-on will collect full inventory data again and that cycle would be continued. The Splunk Add-on for VMware communicates with vCenter Server using network ports and Splunk management ports.

Sender	Receiver	Port number	Description
Scheduler (on the search head)	vCenter server	443	The scheduler uses port 443 to connect to the vCenter Server to verify that the vCenter Server credentials are valid. It also uses this port to discover the number of managed ESXi hosts in the environment.
Splunk Add-on for VMware	Data Collection Node	8089	The Splunk App for VMware connects to the Data Collection Node (DCN) on the default Splunk management port, TCP 8089.

Scheduler	Data Collection Node	8008	When the DCN and Splunk App for VMware have established a connection, the scheduler, which typically runs on the search head, allocates data collection jobs to the DCN on the TCP port 8008. TCP port 8008 is the gateway port. In your environment, if another service uses port 8008, you can configure a different port for communication between the data collection node and the gateway. Data collection nodes do not have to communicate on the same port.
			`[default]`
			`gateway_port = 8008`
			To change the ports for each data collection node individually, set the port in each stanza.

Data Collection Node (DCN)	vCenter Server	443	The DCN communicates with vCenter Server API on port 443 to execute the data collection tasks allocated to it.
Data Collection Node	Splunk indexer	9997	The Data Collection Node uses port 9997 to forward data it has retrieved from the vCenter Server using the API.

After the Splunk Add-on for VMware establishes a connection with a vCenter Server, the DCN uses port 443 to obtain the credentials for vCenter Server. The DCN uses port 443 to determine the kind of data to collect, such as performance, inventory, or hierarchy data. Splunk App for VMware sends information to the data collection nodes using port 8008 about the information they need to collect from a specific vCenter Server system. The DCN retrieves the data from vCenter Server and forwards the data to the Splunk indexer on port 9997.

Control certificate validation for your data collection nodes

Control certificate validation your data collection nodes with the `ta_vmware_config_ssl.conf` file. Use it to enable and disable certificate validation for your DCN. By default, certificate validation is disabled.

1. On your scheduler, navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/default` and copy the `ta_vmware_config_ssl.conf` file.
2. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware` and create a `local` folder.
3. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local` and paste the `ta_vmware_config_ssl.conf` file.
4. Open the `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local/ta_vmware_config_ssl.conf` and set `validate_ssl_certificate` option to `true`.
   ```
   [general]
   validate_ssl_certificate = true
   ```
5. Save your changes.
6. Restart your Splunk platform instance.

For more information, see the About securing inter-Splunk communication section of the *Securing Splunk Enterprise* documentation.

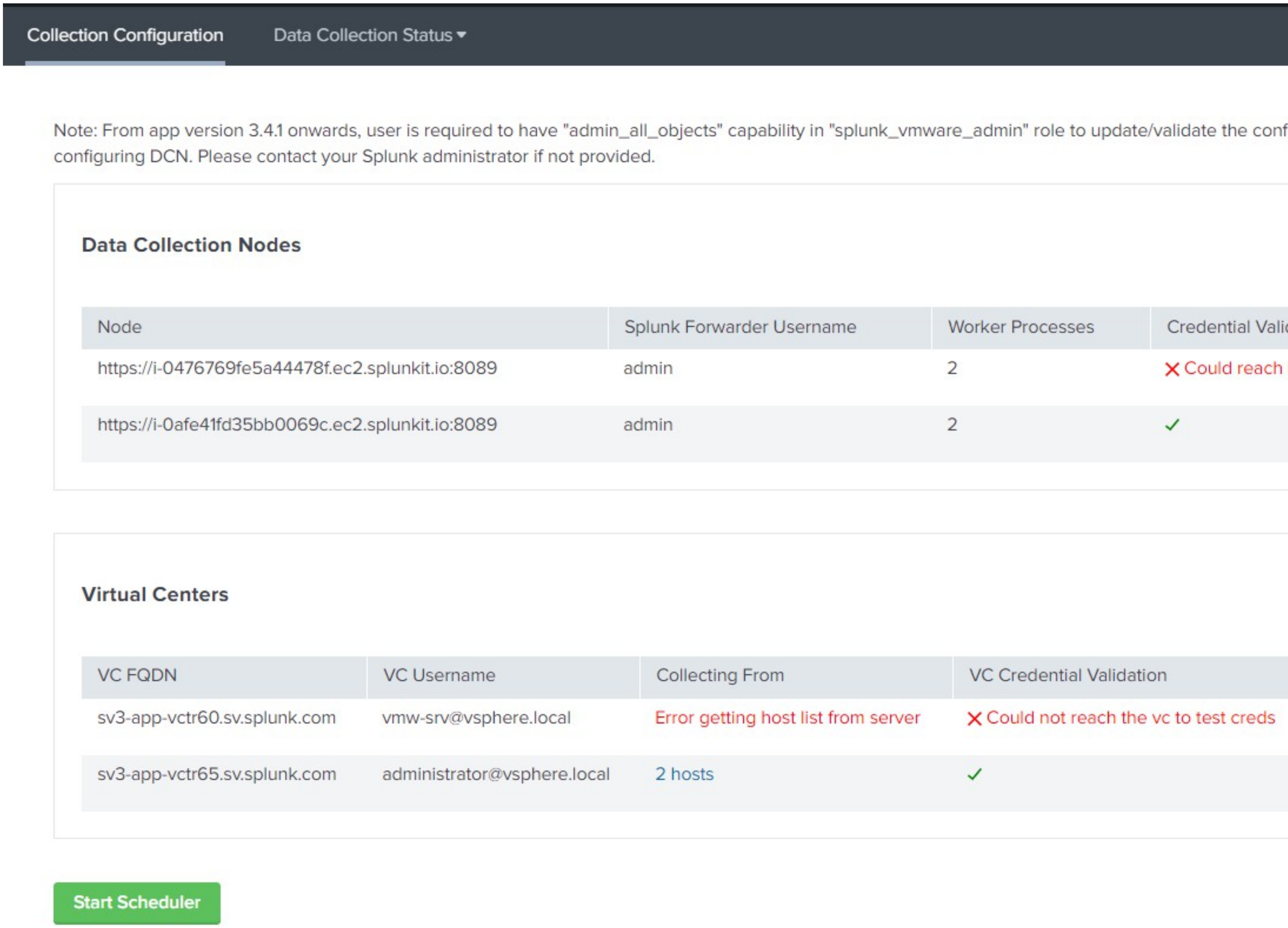
Configure VMX Logs to Syslog

Configure your Splunk platform infrastructure to collect vmware.log files from your VM infrastructure. This configuration provides your Splunk platform deployment with a source of data that lets you audit, troubleshoot and rebuild your VMX configuration files.

1. Navigate to your virtual machine vmx file.
2. Add `vmx.log.destination = "syslog-and-disk"` to your virtual machine vmx file.
3. Name your vm log entry. (Example:`vmx.log.syslogID = vmx[splunkdata]`)
4. Check the log entry in **/var/log/syslog** of your ESXi host to verify the syslog is being forwarded.

Use the Collection Configuration page to add configurations

The Collection Configuration dashboard, on the Scheduler, manages the collection of Data Collection Node (DCN) and Virtual Center data. Register all data collection nodes with the Collection Configuration dashboard in order to collect data from vCenter Server. You must configure each DCN separately with the scheduler.



Note: From app version 3.4.1 onwards, user is required to have "admin_all_objects" capability in "splunk_vmware_admin" role to update/validate the conf configuring DCN. Please contact your Splunk administrator if not provided.

Data Collection Nodes

Node	Splunk Forwarder Username	Worker Processes	Credential Vali
https://i-0476769fe5a44478f.ec2.splunkit.io:8089	admin	2	✗ Could reach
https://i-0afe41fd35bb0069c.ec2.splunkit.io:8089	admin	2	✓

Virtual Centers

VC FQDN	VC Username	Collecting From	VC Credential Validation
sv3-app-vctr60.sv.splunk.com	vmw-srv@vsphere.local	Error getting host list from server	✗ Could not reach the vc to test creds
sv3-app-vctr65.sv.splunk.com	administrator@vsphere.local	2 hosts	✓

Data Collection Node configuration

1. Navigate to the **Collection Configuration** page.
2. Under **Data Collection Nodes**, Click on **Add DCN**.
3. Enter in your **Splunk Forwarder URI**, **Username**, **Password**, and number of **Worker Processes** Data Collection Node configuration settings table

Field	Value
Splunk Forwarder URI	The address or port of the DCN. For example, https://<host_name_or_ip_address_of_DCN>:8089.
Splunk Forwarder Username	admin.
Splunk Forwarder Password	The administrator password. Make sure this password is not the Splunk Enterprise default admin password (changeme).
Worker Processes	Define the number of worker processes you want on the node. This is the number of processes you can run on the data collection node to process the data and forward it to the indexer(s). You can run a maximum of 30 processes per node at the default configuration. The number of worker processes must be one fewer than the number of CPU cores the vCenter Server system granted to the DCN. For example, if the DCN has four CPU cores, the number of worker processes is three.

4. Click **Save**
5. Confirm that you correctly configured the DCN by verifying that the DCN, credential validation, and add-on validation all display a green check.
6. Repeat the steps for each DCN.

Data Collection preferences configuration

Use data collection preferences to allow or block performance metrics for the host, VM, cluster and resourcepool.

- **Virtual Machine Metric Allowlist**, **Virtual Machine Metric Denylist**, **Host Metric Allowlist** and **Host Metric Denylist** options are shown and affected only when **hostvmperf** task is enabled from the Collection Configuration page.

- **Cluster Metric Allowlist**, **Cluster Metric Denylist**, **ResourcePool Metric Allowlist** and **ResourcePool Metric Denylist** options are shown and affected only when **otherperf** is enabled from the Collection Configuration page.

1. Navigate to the **Collection Configuration** page.
2. Select **Data Collections preferences**.
3. Enter your metric preferences:

Field	Value
VM Metric Allowlist	Collects data of VM performance metrics matched with the regex, by default it will collect all metrics unless specified as regex. For example `.*_cpu_.*`, `.*_net_.*`
VM Metric Denylist	Collects data of VM performance metrics not matched with the regex, by default it will collect all metrics unless specified as regex. For example `.*mem.*`
Host Metric Allowlist	Collects data of Host performance metrics matched with the regex, by default it will collect all metrics unless specified as regex. For example `^p_average.*`, `.*_cpu_.*`
Host Metric Denylist	Collects data of Host performance metrics not matched with the regex, by default it will collect all metrics unless specified as regex. For example `.*_cpu_.*`, `.*_disk_.*`

Field	Value
Cluster Metric Allowlist	Collects data of Cluster performance metrics matched with the regex, by default it will collect all metrics unless specified as regex. For example .*_(clusterServices|cpu).*, default value is ^p_(?!average_cpu_reservedCapacity_megaHertz).*_(clusterServices|cpu).*
Cluster Metric Denylist	Collects data of Cluster performance metrics not matched with the regex, by default it will collect all metrics unless specified as regex. For example `p_average_cpu_reservedCapacity.*`
ResourcePool Metric Allowlist	Collects data of ResourcePool performance metrics matched with the regex, by default it will collect all metrics unless specified as regex. For example `.*_cpu_.*`
ResourcePool Metric Denylist	Collects data of ResourcePool performance metrics not matched with the regex, by default it will collect all metrics unless specified as regex. For example `.*_cpu_.*`

4. Click **Save**.

Virtual Center configuration

Add a vCenter Server system as a source of data in your environment.

1. Navigate to the **Collection Configuration** page.
2. Under **Virtual Centers**, click **Add VC**.
3. Enter in your **Virtual Center FQDN**, **VC Username**, **VC Password**, and select the **Collect from all hosts** checkbox.

Field	Value
Virtual Center FQDN	The fully-qualified domain name for the vCenter server. For example, `test-vcenter100.example.com`
VC Username	The user name that you configured in vCenter Server for Splunk Enterprise. Use the format `username@domain` if the user is an Active Directory account.
VC Password	The password that you configured in vCenter Server for Splunk Enterprise.

4. (Optional) Select the **Collect from all hosts** checkbox.
5. (Optional) Enter in your **VC Splunk Forwarder URI**, '**VC Splunk Forwarder Username**, 'and **VC Splunk Forwarder Password**.
6. For the initial installation, pull 20 or fewer hosts. If the vCenter Server manages other servers, make sure that **Collect form all hosts** and allowlist-specific hosts are not selected.
7. Click **Save**.
8. Verify that each of the vCenter Server entries displays a green check.
9. Click **Start Scheduler**. The Distributed Collection Scheduler is running when the button label is **Stop Scheduler**.

Test DCN and vCenter Server configurations

1. Approximately ten minutes after you start the scheduler, access the search head and navigate to the Splunk Search field.
2. Type a search string to test data collection.

   `sourcetype=vmware:perf*` OR `sourcetype=vmware:inv:hierarchy`

3. Confirm that the search returns results. Dashboards and some of the other graphics might take up to 60 minutes to populate.

Set performance parameters

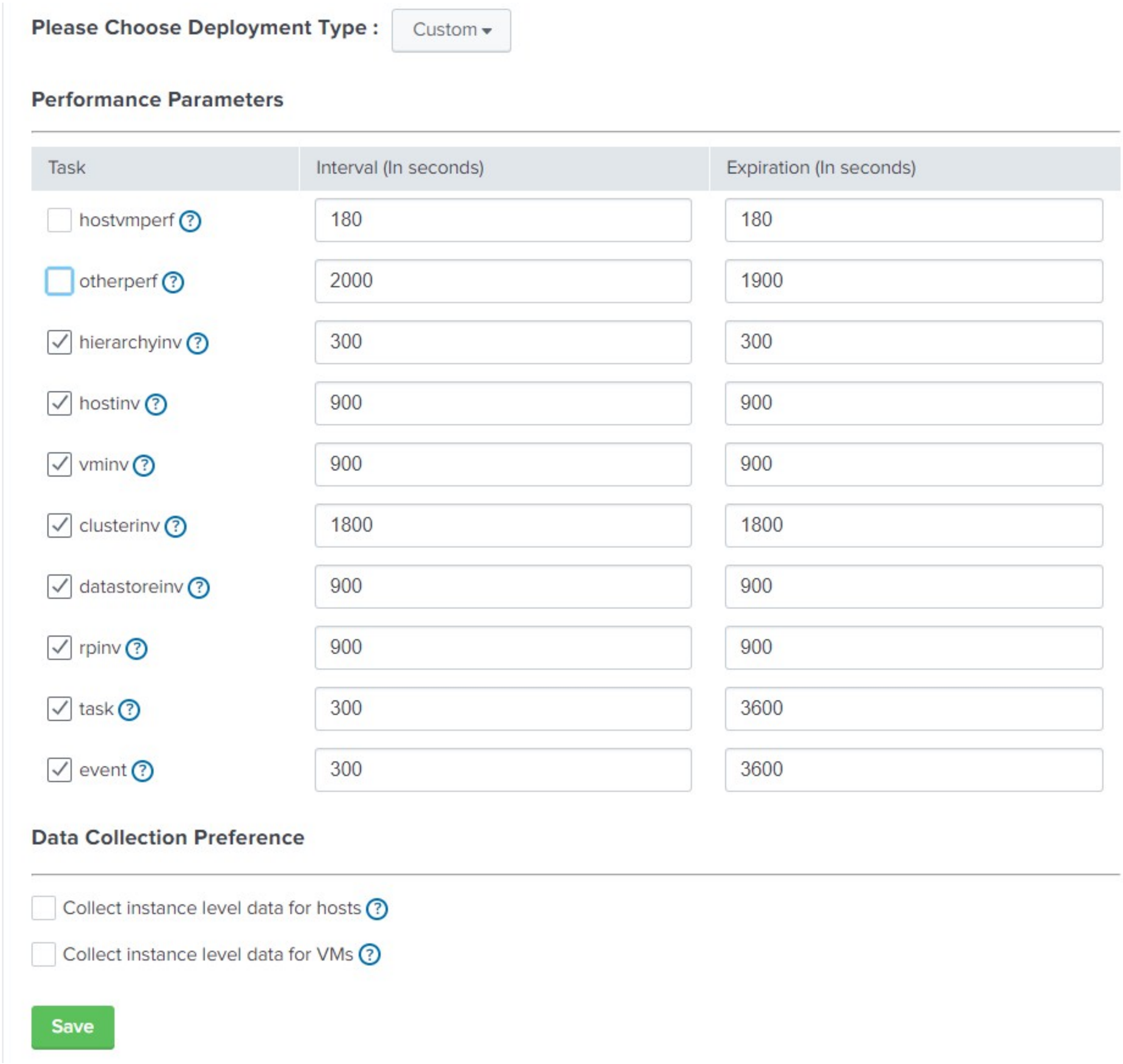
The Splunk Add-on for VMWare contains the ability to use the UI to adjust performance parameters from the **Collection Configuration** page.

The below table lists the default tasks that are required for either your ITSI Virtualization Module deployment, or your VMware App deployment. If you change any default settings for either deployment type, the deployment type will change to a **Custom** deployment type.

Task	ITSI Virtualization Module Deployment	VMware App Deployment
hostvmperf	x	x
otherperf		x
hierarchyinv		x
hostinv	x	x
vminv	x	x
clusterinv		x
datastoreinv	x	x
rpinv		x
task		x
event		x

Use the **Collection Configuration** page to set interval and expiration times for the performance parameters of the Splunk Add-on for VMware. This information can also be adjusted using `ta_vmware_collection.conf` in `$SPLUNK_HOME/etc/apps/TA_vmware/local/`.

1. Navigate to the performance parameter task that you want to adjust.
2. Enter the interval amount in seconds.
3. Enter the expiration amount in seconds
4. Click **Save**.



Please Choose Deployment Type : Custom ▾

Performance Parameters

Task	Interval (In seconds)	Expiration (In seconds)
□ hostvmperf ?	180	180
□ otherperf ?	2000	1900
☑ hierarchyinv ?	300	300
☑ hostinv ?	900	900
☑ vminv ?	900	900
☑ clusterinv ?	1800	1800
☑ datastoreinv ?	900	900
☑ rpinv ?	900	900
☑ task ?	300	3600
☑ event ?	300	3600

Data Collection Preference

□ Collect instance level data for hosts ?

□ Collect instance level data for VMs ?

Collect instance level data

In a "VMware" deployment type, data will not be collected at the instance level. In an **ITSI** deployment type, data will be collected at the instance level for only ITSI specific tasks.

With these option enabled, the VMWare add-on collects performance data of all instances of resources such as CPU, disk, datastore for hosts. e.g Each Core is an instance for the CPU resource, Each Disk Id is an instance for the Disk resource, Each Datastore Id is an instance for the Datastore resource. In the VMWare app the aggregated value returned from the vCenter API is used for performance data.

If you want to collect instance level data, navigate to the **Data collection preference** section of the **Collection Configuration** page, and check the **Collect instance level data for hosts** and the **Collect instance level data for VMs**, depending on whether you want to collect instance level data for your hosts and VMs.

Configure Splunk Add-on for VMware performance data collection

This topic discusses how to improve the performance of the vCenter server when you see performance issues during data collection.

You can limit the processing (reduce the memory and cpu load) on the vCenter server during data collection when you see performance issues with your vCenter server. How performance data is collected in the Splunk Add-on for VMware is specified in the file `ta_vmware_collection.conf`. The parameter `perf_format_type` is set to one of two modes:

- csv mode. The response from the ESXi host when collecting performance data is parsed by vCenter. Performance data is collected by the Splunk App for VMware, from vCenter, by default, using csv mode.
- normal mode. The response from the ESXi host when collecting performance data is parsed by the data collection nodes. This reduces the load on vCenter.

To change modes, edit a local version of `etc/apps/Splunk_TA_vmware/default/ta_vmware_collection.conf`, and change the value of `perf_format_type` to `normal`. Processing performance data is now done on the data collection node.

Change data collection node capabilities and log levels

Change DCN capabilities

At the node level, `hydra_node.conf` contains the capabilities field. The Collection Configuration page sets the capabilities of the workers on the data collection nodes. You can change the capabilities for a node.

The capabilities in `hydra_node.conf` can be changed by the data collection node to only include certain tasks. For example, if two data collection nodes are specified in `hydra_node.conf`, one data collection node can require more power and more memory to process more intensive tasks than the other data collection node. The capabilities are specified by the following lines in `hydra_node.conf`:

```
[dcn1:8089]
capabilities = hostinv, vminv
[dcn2:8089]
capabilities = task, event
```

1. Create a local version of `hydra_node.conf`.

2. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local/hydra_node.conf` on the scheduler node to adjust the capabilities.

```
[default]
â ¨gateway_port = 8008
â ¨capabilities = * â ¨
```

Change DCN log levels

To troubleshoot your environment, you can set the field `worker_log_level` in `hydra_node.conf` for a data collection node.

1. On the Collection Configuration page, create a local version of `hydra_node.conf`.
2. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local/hydra_node.conf` to set the log level of for all data collection nodes. The default log level for a data collection node is INFO. The most verbose logging level is DEBUG.

Example:

```
[default]
â ¨gateway_port = 8008
â ¨capabilities = * â ¨
worker_log_level = DEBUG
```

Install the Splunk Add-on for VMware in a cloud environment

This table outlines a distributed deployment installation of the Splunk Add-on for VMware on a cloud environment.

To collect the data from your VMware environment you have to install the packages on your on-premises data collection node, scheduler, and log forwarder. Follow the steps in Install the Splunk Add-on for VMware in on-premises environment for the installation steps for data collection node, scheduler, and log forwarder components.

Splunkbase Add-on	Component	Search head	Scheduler (DCS)	Indexer	Data Collection Node (DCN)	Dedicated ESXi log forwarder	Dedicated vCenter log forwarder
Splunk Add-on for VMware	Splunk_TA_vmware SA-Hydra		X		X		
Splunk Add-on for ESXi Logs	Splunk_TA_esxilogs	X				X	
Splunk Add-on for vCenter Logs	Splunk_TA_vcenter	X					X
Splunk Add-on for VMware Indexes	SA-VMWIndex			X			
Splunk Add-on for VMware Extractions	TA-VMW-FieldExtractions	X					

Install the Splunk Add-on VMware and prerequisite add-ons on the cloud environment

The packages included in Splunk Add-on for VMware (SA-Hydra, Splunk_TA_vmware) aren't required in cloud environments (Indexer/Search Head). Follow these steps to install the prerequisite add-ons on the respective tier on the Splunk cloud environment.

1. Log in to your search head.
2. On the Splunk Web home page, click **Find More Apps**.
3. Search for these add-ons and click **Install**.
   - ♦ Splunk Add-on for VMware ESXi Logs
   - ♦ Splunk Add-on for vCenter Logs
   - ♦ Splunk Add-on for VMware Indexes
   - ♦ Splunk Add-on for VMware Extractions
4. Enter your Splunk.com login credentials, read and accept the terms and conditions, and click **Login and Install**.
5. Go to **Apps** > **Manage Apps** to review the installed app on the **Apps** page.

Upgrade

Upgrade to the Splunk Add-on for VMware 4.0.2

If you have not removed uuid.py from Scheduler or DCN, you'll get the following error: [Error "ImportError: bad magic number in 'uuid': b'\x03\xf3\r\n'" in hydra logs.]. The error is described in Troubleshoot the Splunk Add-on for VMware and requires you to manually delete the pyc file.

Step 1: Download the files from Splunkbase

1. Download the Splunk Add-on for for VMware version 4.0.2 from Splunkbase to a location in your environment.
2. Download the Splunk OVA for VMware version 4.0.2 from Splunkbase to a location in your environment.

Step 2: Upgrade scheduler

You can upgrade the scheduler using a script or manually.

Upgrade using a script

Make sure the splunk_vmware_admin role has admin_all_objects capability.

1. Download the script file: File:Upgade from VMware Event TA 400 401 to 402.zip.
2. Unzip it to get the upgrade script.
3. Put the upgrade script on the scheduler machine.
4. Stop the scheduler. You can stop the scheduler in the **Collection Configuration** page of your scheduler machine.
5. Stop Splunk on the scheduler instance.
6. Extract the contents of the Splunk Add-on for VMware to the `$SPLUNK_HOME/etc/apps` directory. Extracting the package contents overwrites the Splunk_TA_vmware and SA-Hydra packages.
7. Go to `$SPLUNK_HOME/etc/apps` and remove the following directories:
    1. SA-VMWIndex
    2. TA-VMW-FieldExtractions
    3. Splunk_TA_vcenter
    4. Splunk_TA_esxilog
8. Run the upgrade script using Python. Use the following command to run the script:

```
$SPLUNK_HOME/bin/splunk cmd python upgrade_script_event_TA.py
```

You'll see a message saying that the Add-on upgraded successfully. In case of errors, refer to the upgrade_event_TA.log file in the `$SPLUNK_HOME/var/log/splunk` directory.

Upgrade manually

1. Stop the scheduler. You can stop the scheduler in the **Collection Configuration** page of your scheduler machine.
2. Stop Splunk on the scheduler instance.
3. Extract the contents of the Splunk Add-on for VMware to the `$SPLUNK_HOME/etc/apps` directory. Extracting the package contents overwrites the Splunk_TA_vmware and SA-Hydra packages.

4. Go to $PLUNK_HOME/etc/apps and remove the following directories:
    1. SA-VMWIndex
    2. TA-VMW-FieldExtractions
    3. Splunk_TA_vcenter
    4. Splunk_TA_esxilog
5. In the `$SPLUNK_HOME/etc/apps` directory, replace the present words in the ta_vmware_collection.conf file with the following replacement words in this table:

Parameter name in Splunk Add-on for VMware version 4.0.1	Parameter name in Splunk Add-on for VMware version 4.0.2
managed_host_whitelist	managed_host_includelist
managed_host_blacklist	managed_host_excludelist
vm_metric_whitelist	vm_metric_allowlist
vm_metric_blacklist	vm_metric_denylist
host_metric_whitelist	host_metric_allowlist
host_metric_blacklist	host_metric_denylist
cluster_metric_whitelist	cluster_metric_allowlist
cluster_metric_blacklist	cluster_metric_denylist
rp_metric_whitelist	rp_metric_allowlist
rp_metric_blacklist	rp_metric_denylist
vm_instance_whitelist	vm_instance_allowlist
vm_instance_blacklist	vm_instance_denylist
host_instance_whitelist	host_instance_allowlist
host_instance_blacklist	host_instance_denylist
cluster_instance_whitelist	cluster_instance_allowlist
cluster_instance_blacklist	cluster_instance_denylist
rp_instance_whitelist	rp_instance_allowlist
rp_instance_blacklist	rp_instance_denylist
perf_entity_blacklist	perf_entity_denylist

Step 3: Upgrade forwarder (DCN)

> Make sure '''splunk_vmware_admin''' role has '''admin_all_objects''' capability.

1. Stop the Splunk on DCN machine.
2. Extract the contents of the Splunk add-on for VMware to the `$SPLUNK_HOME/etc/apps` directory. Extracting the package contents overwrites the add-on packages installed previously.
3. Go to `$PLUNK_HOME/etc/apps` and remove the following directories:
    1. SA-VMWIndex
    2. TA-VMW-FieldExtractions
    3. If you are forwarding the vCenter logs to the indexer directly, remove the **Splunk_TA_vcenter** directory. If you are forwarding the ESXi logs to the indexer directly, remove the **Splunk_TA_esxilogs** directory.

Step 4: Upgrade indexer (Optional)

1. Enable maintenance mode on cluster master node.
2. Navigate to the **apps** folder for your deployment (**etc/apps** for non-indexer cluster deployments, and **etc/master-apps** for indexer clustering deployments) and overwrite **Splunk_TA_esxilogs**, **splunk_TA_vcenter**, and **SA-VMWIndex** on the cluster master node with new versions.
3. If forwarding VC Logs and ESXi logs to DCN machine, remove the **Splunk_TA_vcenter** directory. If you are forwarding the ESXi logs to the DCN, remove the **Splunk_TA_esxilogs** directory.
4. Push configuration bundle from cluster master node if you set up an indexer cluster.

Step 5: Upgrade the forwarder on your vCenter server(s)

This applies only to Windows-based vCenter servers - not vCSA.

Stop your Splunk forwarder.

1. Extract the contents of the Splunk Add-on for VMware package to `splunkforwarder/etc/apps`. This overwrites the existing Splunk_TA_vcenter package.
2. Remove the following packages from splunkforwarder/etc/apps:
    1. Splunk_TA_vmware
    2. SA-Hydra
    3. TA-VMW-FieldExtractions
    4. Splunk_TA_esxilogs
3. Confirm that in `etc/system/local/output.conf`, server entries to forward vclogs are present.
4. Restart your Splunk forwarder.

Step 6: Upgrade search head

For search head cluster deployments

1. Extract the add-on package components to `etc/shcluster/apps`.
2. Remove Splunk_TA_vmware and SA-VMWIndex from `etc/shcluster/apps/` from your deployer.
3. Push the app bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer does not restart the search head cluster members, perform a rolling restart.

For dedicated search head deployments

1. Stop Splunk on the search head.
2. Extract the add-on package components to `etc/apps`.
3. Remove the Splunk_TA_vmware and SA-VMWIndex packages from `etc/apps`.
4. Restart Splunk on the search head.

Step 7: Start the scheduler and the DCN

1. Start Splunk on the DCN machine.
2. Start Splunk on the scheduler machine.
3. Navigate to the **Collection Configuration** page of the Splunk Add-on for VMware on your scheduler.
4. Click the "Start Scheduler" button to start data collection.

Validate the Splunk App for VMware upgrade on your search head

Validate that you correctly upgraded the Splunk App for VMware to the latest version and that the app can collect data.

1. Log in to the Splunk App for VMware on your search head.
2. When the app displays the **Splunk for VMware Setup** page, select the **Delete all deprecated Add-ons** checkbox under **Disable/delete old add-ons**. The app removes all legacy add-ons from the installation. This removes saved searches of SA-VMW-Performance that are no longer in use.
3. Save your configurations, and restart your Splunk platform deployment.

Manually remove legacy add-ons

If you launched Splunk App for VMware but did not check **Delete all deprecated Add-ons** on the setup page, you can manually remove the legacy add-ons from your installation.

1. Stop the Splunk platform on your search head.
2. Delete the `hydra_job.conf` file in the `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local` folder on the Splunk Search head.
3. Remove the `SA-VMW-Licensecheck` folder from the `$SPLUNK_HOME/etc/apps` folder on your Splunk search head. Do this for each server upon which you installed the Splunk App for VMware.
4. The below table shows the specific legacy add-ons, located in the `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local` folder of the Splunk App for VMware, to delete when upgrading:

- `DA-VMW-HierarchyInventory`
- `DA-VMW-LogEventTask`
- `DA-VMW-Performance`
- `SA-VMW-Licensecheck`

- Restart your Splunk platform.

Additional information

See "Platform and Hardware Requirements" in this manual for supported Splunk platform versions for this release. See "How to upgrade Splunk Enterprise" to upgrade to a new version of the Splunk platform.

For information on upgrading from tsidx namespaces to data model acceleration, see the "Upgrade from tsidx namespaces to data model acceleration" section of the troubleshooting section of this manual.

Upgrade the Splunk Add-on for VMware from v4.0.2 to v4.0.4

These steps cover upgrading from Splunk Add-on for VMware v4.0.2 to v4.0.4 only. If you are using a version previous to v4.0.2, follow the steps to upgrade to the Splunk Add-on for VMware 4.0.2. You can then follow these steps to upgrade to v4.0.4.

Step 1: Upgrade the scheduler

1. Stop the scheduler. You can stop the scheduler on the **Collection Configuration** page of your scheduler machine.
2. Stop Splunk on the scheduler instance.

3. Download the Splunk Add-on for VMware from Splunkbase.
4. Extract the components of Splunk Add-on for VMware to the $SPLUNK_HOME/etc/apps directory. Extracting the package contents overwrites the Splunk_TA_vmware and SA-Hydra components.

Step 2: Upgrade the forwarder data collection node

1. Stop Splunk on the data collection node machine.
2. Download these add-ons from Splunkbase:
   - ♦ Splunk Add-on for VMware (contains the Splunk_TA_vmware and SA-Hydra packages)
   - ♦ Splunk Add-on for vCenter Logs (contains the Splunk_TA_vcenter package)*
   - ♦ Splunk Add-on for VMware ESXi Logs (contains the Splunk_TA_esxilogs package)*
3. Extract the package components to the $SPLUNK_HOME/etc/apps directory. Extracting the package components overwrites Splunk_TA_vmware, SA-Hydra, Splunk_TA_vcenter, and Splunk_TA_esxilogs packages.

* Only download if you are directly forwarding the logs to the data collection node.

Step 3: Upgrade the indexer

1. Enable maintenance mode on the cluster master node for the indexer cluster or stop Splunk on the indexer machine for non-cluster indexers.
2. Download these packages from Splunkbase:
   - ♦ Splunk Add-on for VMware Indexes (contains the SA-VMWIndex package)
   - ♦ Splunk Add-on for vCenter Logs (contains the Splunk_TA_vcenter package)
   - ♦ Splunk Add-on for VMware ESXi Logs (contains the Splunk_TA_esxilogs package)
3. Extract the package components:
   - ♦ For clustered indexer deployment, extract the package components to the $SPLUNK_HOME/etc/master-apps directory on the cluster master node and push configuration bundle from cluster master node.
   - ♦ For non-clustered indexer deployment, extract the package components to the $SPLUNK_HOME/etc/apps directory on each indexer node.

Step 4: Upgrade the search head

1. If you are using non-clustered search heads, stop Splunk on the search head.
2. Download these packages from Splunkbase:
   - ♦ Splunk Add-on for VMware Extractions (contains the TA-VMW-FieldExtractions package)
   - ♦ Splunk Add-on for vCenter Logs (contains the Splunk_TA_vcenter package)
   - ♦ Splunk Add-on for VMware ESXi Logs (contains the Splunk_TA_esxilogs package)
3. Extract the package components:
   - ♦ For clustered search head deployment, extract the components from the packages to the $SPLUNK_HOME/etc/shcluster/apps directory on the deployer node and push the bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer doesn't restart the search head cluster members, perform a rolling restart.
   - ♦ For non-clustered search heads, extract the components from the packages to the $SPLUNK_HOME/etc/apps directory on each search head node.

Step 5: Upgrade the dedicated ESXi log forwarder

1. Stop Splunk on the dedicated log forwarder instance.
2. Download the Splunk Add-on for VMware ESXi Logs from the Splunkbase.
3. Extract the package components to the $SPLUNK_HOME/etc/apps directory.

Step 6: Upgrade the dedicated vCenter log forwarder

1. Stop Splunk on the dedicated log forwarder instance.
2. Download the Splunk Add-on for vCenter Logs from the Splunkbase.
3. Extract the package components to the $SPLUNK_HOME/etc/apps directory.

Step 7: Start Splunk and data collection

1. Start Splunk on all the respective nodes (data collection node, scheduler, forwarders).
2. Navigate to the **Collection Configuration** page of the Splunk Add-on for VMware on your scheduler.
3. Click **Start Scheduler** to start data collection.

Upgrade the Splunk Add-on for VMware from v3.4.5 to v4.0.0

These steps cover upgrading from Splunk Add-on for VMware from version 3.4.5 to version 4.0.0.

Upgrade your scheduler to v4.0.0

Follow these steps on the scheduler machine.

1. Stop your scheduler by selecting **Stop Scheduler** from the **Collection Configuration** page of the add-on.
2. Stop Splunk.
3. Overwrite splunk_TA_vmware and SA-Hydra packages with new versions packaged in Splunk Add-on for VMware v4.0.0 build.
4. Delete these other apps: SA-VMNetAppUtils, SA-VMWIndex, and TA-VMW-FieldExtractions.
5. Remove suds directory, uuid.py and uuid.pyc files from the Splunk_TA_vmware/bin/ directory.
6. Remove uuid.py and uuid.pyc files from the SA-Hydra/bin/hydra/ directory.
7. (Optional) Remove SA-Hydra/appserver directory.

Upgrade your data collection node

Follow these steps on the data collection node (DCN) machine.

1. Stop Splunk.
2. Overwrite versions of Splunk_TA_vmware, Splunk_TA_esxilogs, Splunk_TA_vcenter and SA-Hydra packages on each data collection node with 4.0.0 versions. #Delete these other apps: SA-VMNetAppUtils, SA-VMWIndex, and TA-VMW-FieldExtractions.
3. Remove suds directory, uuid.py, and uuid.pyc files from the Splunk_TA_vmware/bin/ directory.
4. Remove uuid.py and uuid.pyc files from the SA-Hydra/bin/hydra/ directory.
5. (Optional) Remove SA-Hydra/appserver directory.

Upgrade the Indexer

Follow these steps on the indexer machine.

1. Enable maintenance mode on the cluster master node for the indexer cluster or stop Splunk on the indexer machine for non-cluster indexers.
2. Remove SA-Hydra, SA-VMNetAppUtils, Splunk_TA_vmware, and TA-VMW-FieldExtractions directories, if present.

3. If you aren't forwarding the data from forwarder then download the Splunk Add-on for VMWare version 4.0.0 from Splunkbase and extract these packages:
    - Splunk_TA_vcenter
    - Splunk_TA_esxilogs
    - SA-VMWIndex
4. Extract the package components according to your deployment type:
    - For clustered indexer deployment, extract the package components to the $SPLUNK_HOME/etc/master-apps directory on the cluster master node and push configuration bundle from cluster master node.
    - For non-clustered indexer deployment, extract the package components to the $SPLUNK_HOME/etc/apps directory on each indexer node.

Upgrade the search head

Follow these steps on the search head machine.

1. If you are using non-clustered search heads, stop Splunk on the search head.
2. (Optional) Remove the SA-Hydra/appserver/ directory, if present.
3. Download the Splunk Add-on for VMWare version 4.0.0 from Splunkbase and extract these packages:
    - Splunk_TA_esxilogs
    - Splunk_TA_vcenter
    - TA-VMW-FieldExtractions
4. Extract the package components according go your deployment type:
    - For clustered search head deployment, extract the components from the packages to the $SPLUNK_HOME/etc/shcluster/apps directory on the deployer node and push the bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer doesn't restart the search head cluster members, perform a rolling restart.
    - For non-clustered search heads, extract the components from the packages to the $SPLUNK_HOME/etc/apps directory on each search head node.

Upgrade the dedicated ESXi log forwarder

Follow these steps on the dedicated ESXi log forwarder machine.

1. Stop Splunk on the dedicated log forwarder instance.
2. Download the Splunk Add-on for VMWare version 4.0.0 from Splunkbase.
3. Extract the Splunk_TA_esxilogs package components to the $SPLUNK_HOME/etc/apps directory.

Upgrade the dedicated vCenter log forwarder

Follow these steps on the dedicated vCenter log forwarder machine.

1. Stop Splunk on the dedicated log forwarder instance.
2. Download the Splunk Add-on for VMWare version 4.0.0 from Splunkbase.
3. Extract the Splunk_TA_vcenter package components to the $SPLUNK_HOME/etc/apps directory.

Start Splunk and data collection

1. Start Splunk on all the respective nodes (data collection node, scheduler, forwarders).
2. Navigate to the **Collection Configuration** page of the Splunk Add-on for VMware on your scheduler.
3. Select **Start Scheduler** to start data collection.

Reference

Troubleshoot the Splunk Add-on for VMware

Data collection issues

Gaps in data collection

Gaps in data collection or slow data collection (example: data only coming in equal or greater to every 20 minutes) sometimes requires a restart of your scheduler. Any updates to `ta_vmware_collections.conf` requires a restart of the scheduler to take effect. Collection configurations using the UI do not require a restart of the scheduler.

vCenter connectivity issues

The Splunk Add-on for VMware cannot make read-only API calls to vCenter Server systems

Inability to make read-only API calls means that you do not have the appropriate vCenter Server service login credentials for each vCenter Server. Obtain vCenter Server service login credentials for each vCenter server.

The Splunk Add-on for VMware is not receiving data

If you have configured vCenter Server 5.0 but no data is coming in, the vCenter Server 5.0 and 5.1 are missing WSDL files that are required for Splunk Add-on for VMware to make API calls to vCenter Server.

◊ reflect-message.xsd
◊ reflect-types.xsd

Resolve this issue by installing the missing VMware WSDL files as documented in the vSphere Web Services SDK WSDL workaround in the VMware documentation. Note that the `programdata` folder is typically a hidden folder.

The DCNs are forwarding data using index=_internal tests, but Splunk App for VMware is not collecting any API data

API data collection issues are typically caused by one of two issues:

- Network connectivity issues from the Scheduler to the DCNs.
- You have not changed the DCN admin account password from its default value.

To resolve this issue:

1. In the Splunk Add-on for VMware **Collection Configuration** page, verify the accuracy of the settings in the collection page.
2. Verify that the `admin` password for each DCN is not set to `changeme`.
3. Verify that each DCN has a fixed IP address. If Splunk App for VMware uses DCN host names instead of fixed IP addresses, verify that DNS lookups resolve to the correct IP addresses.

Hydra scheduler proxy access error

If you attempt to use a proxy server to connect to Splunk Web and receive the following proxy error message:

```
URLError: <urlopen error Tunnel connection failed: 403 Proxy Error>
```

You will also see the following error message in your log files:

```
hydra_scheduler_ta_<ip address>_scheduler_nidhogg.log
```

The hydra scheduler checks Splunk Web's proxy settings, and is trying to connect to a data collection node (DCN) through the proxy server. You cannot install a scheduler if you use a proxy server for Splunk Web.

Fix this problem by deploying and setting up your Splunk Enterprise instance inside the same network as your data collection nodes without the use of a proxy server.

Permissions in vSphere

Splunk Add-on for VMware must use valid vCenter Server service credentials to gain read-only access to vCenter Server systems using API calls. The account's vSphere role determines access privileges.

The following sections list the permissions for the vCenter server roles for all of the VMware versions that Splunk App for VMware supports.

Permissions to use your own syslog server

Best practice dictates that use your own syslog server, and that you install a Splunk Enterprise forwarder on the server to forward syslog data. Use these permissions to collect data from the ESXi hosts using your own syslog server. These system-defined privileges are always present for user-defined roles.

Permission
System.Anonymous
System.Read
System.View

Permissions to use an intermediate forwarder

Use these permissions if you configure your ESXi hosts to forward syslog data to one or more intermediate Splunk Enterprise forwarders. Use the vSphere client to enable the syslog firewall for the specific hosts. Note that in vSphere 5.x you do not need to add permissions beyond the default ones vSphere provides when creating a role.

Permission
System.Anonymous
System.Read
System.View
Host.Config.AdvancedConfig

Splunk add-on for VMware sets SSL for WebUI as Default

Disable WebUI SSL in the Splunk Add-on for VMware to prevent **web.conf** from overriding your deployment's SSL settings. Navigate to `$SPLUNK_HOME/etc/system/local/` and make the following change to `web.conf`

```
[settings]
enableSplunkWebSSL = false
```

Esxilog issue

Problem

Not getting esxilogs while forwarding it to indexers which are in a cluster.

Or on indexers, you see the following ERROR message in splunkd.log:

```
ERROR AggregatorMiningProcessor - Uncaught Exception in Aggregator, skipping an event:
Can't open DateParser XML configuration file
"/opt/splunk/etc/apps/Splunk_TA_esxilogs/default/syslog_datetime.xml": No such file or
directory - data_source="/data/log_files/syslog/<hostname>.log", data_host="<hostname>",
data_sourcetype="vmw-syslog"
```

Cause

While esxilogs are directly forwarded to indexers (which are in cluster), splunkd.log on indexers will show the above error.

Reason: Splunk is not able to find custom datetime (syslog_datetime.xml) file which is used to extract dates and timestamps from events.

The following parameter is set for this in props.conf.

```
DATETIME_CONFIG = /etc/apps/Splunk_TA_esxilogs/default/syslog_datetime.xml
```

As indexers are in cluster, Splunk_TA_esxilogs on indexers would be installed under slave-apps (/etc/slave-apps/) hence above path would not exist.

Resolution

1. On cluster-master, Create local directory in the $SPLUNK_HOME/etc/master-apps/Splunk_TA_esxilogs directory, if not present.
2. If not present, create props.conf file in the `$SPLUNK_HOME/etc/master-apps/Splunk_TA_esxilogs/local directory` and add the below stanza and configuration to it:

   ```
   [vmw-syslog]
   DATETIME_CONFIG = /etc/slave-apps/Splunk_TA_esxilogs/default/syslog_datetime.xml
   ```
3. Push the bundle on indexers.

Inventory data fields are not getting extracted using spath command

Issue

The Splunk Add-on for VMware collects the VMware infrastructure inventory data. Inventory data can contain JSON content that exceeds the default spath command character limit of 5000 characters.

Resolution

If you're using the spath command to extract inventory data and the event contains more than 5000 characters, see Update the default character count limitations for the search commands.

Enable cluster DRS service error: lookup table "TimeClusterServicesAvailability" is empty on some dashboards

Problem

Here are troubleshooting steps for enabling cluster DRS service if you see the error `Lookup table "TimeClusterServicesAvailability" is empty` on the following cluster compute resource related dashboards:

- Capacity Planning for Clusters-CPU Headroom
- Capacity Planning for Clusters-Memory Headroom
- Capacity Planning (Clusters)
- Cluster details

If you do not want to enable cluster DRS service, ignore the error.

Cause

The add-on is not able to get following required metrics, so the TimeClusterServicesAvailability lookup is empty:

- `p_average_clusterServices_effectivecpu_megaHertz`
- `p_average_clusterServices_effectivemem_megaBytes`

Resolution

Enable cluster DRS service of the configured vCenter to get the required metrics:

- Log in to configured vCenter using vsphere client.
- Navigate to **Home** > **Inventory** > **Hosts and Clusters**.
- Right click on **Cluster**.

1. Open **Cluster** in Settings
2. Go to Cluster features and click **Turn on vSphere DRS**.

Troubleshoot the error "ValueError: unsupported pickle protocol: 3" in hydra worker logs

Problem

The Splunk add-on for VMware is unable to run the hydra worker script and following logs in hydra worker:

```
ERROR [ta_vmware_collection_worker://worker_process2:28696] Problem with hydra worker
ta_vmware_collection_worker://worker_process2:28696: unsupported pickle protocol: 3
Traceback (most recent call last):
File "/home/splunker/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_worker.py", line 622, in run
  self.establishMetadata()
File "/home/splunker/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_worker.py", line 64, in establishMetadata
  metadata_stanza = HydraMetadataStanza.from_name("metadata", self.app, "nobody")
File "/home/splunker/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 610, in from_name
```

```
  host_path=host_path)
File "/home/splunker/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 533, in get
  return self._from_entity(entity)
File "/home/splunker/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 345, in _from_entity
  obj.from_entity(entity)
File "/home/splunker/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 903, in from_entity
  super(SplunkAppObjModel, self).from_entity(entity)
File "/home/splunker/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 661, in from_entity
  return self.set_entity_fields(entity)
File "/home/splunker/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
  from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
File "/home/splunker/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
  obj = cPickle.loads(b64decode(val))
ValueError: unsupported pickle protocol: 3
```

Cause

The add-on is unable to deserialize the python object that is serialized using another python version than the current python version on which add-on is running. This usually happens when the add-on that was running on Python 3, is running on Python 2. Python 2 is unable to deserialize the python object serialized by Python 3.

Resolution

1. Stop the Scheduler from Collection Configuration page.
2. Stop Splunk on DCN.
3. On DCN, go to `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local` and remove the following files:
    1. ta_vmware_cache.conf
    2. hydra_session.conf
    3. hydra_metadata.conf
4. Start Splunk on DCN.
5. Start the Scheduler from Collection Configuration page.

Troubleshoot the error "ImportError: bad magic number in 'uuid': b'\x03\xf3\r\n'" in hydra scheduler logs

Problem

The Splunk add-on for VMware is unable to run the hydra scheduler script and the following logs in hydra scheduler, so no jobs are assigned.

```
Traceback (most recent call last):
 File "ta_vmware_collection_scheduler.py", line 20, in <module>
   from hydra.hydra_scheduler import HydraScheduler, HydraCollectionManifest, HydraConfigToken
 File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 11, in <module>
   import uuid
ImportError: bad magic number in 'uuid': b'\x03\xf3\r\n'
```

Cause

This error is caused by the `uuid.pyc` file that is compiled on Splunk 7.2.x, Splunk 7.3.x or Splunk 8.x (Python version 2) and is being run on Splunk version 8.x (Python version 3).

Resolution

1. Stop Scheduler from Collection Configuration page.
2. Stop Splunk on Scheduler and DCN machines.

3. Remove all the .pyc files existing in following directory on all the DCN machines and scheduler.
    1. `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin`
    2. `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin/vim25`
    3. `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin/ta_vmware`
    4. `$SPLUNK_HOME/etc/apps/SA-Hydra/bin/hydra`
4. Start Splunk on DCN machine
5. Start Splunk on Scheduler machine
6. Start Scheduler from Collection Configuration page.

Troubleshoot issue in cluster performance data collection caused by collection interval mismatch across configured vCenter

Problem

The add-on is unable to get cluster performance data. The following query doesn't return any results:

```
index="vmware-perf" source="VMPerf:ClusterComputeResource" | dedup sourcetype | table sourcetype
```

Also, you get the following error on the search head in `hydra_worker_ta_vmware_collection_worker_*.log`:

```
2020-04-23 16:12:27,883 ERROR [ta_vmware_collection_worker://worker_process20:19296] Server raised fault:
'A specified parameter was not correct: interval'
```

Cause

The collection interval is set to different values across the configured vCenters. For example, if the VC1 collection interval is 5 minutes, and VC 2 is set to 3 minutes, then it's possible that the add-on fetches cluster performance data for only one vCenter at a time.

This is because the add-on script caches the collection interval and uses it when fetching cluster performance data. If a vCenter has a different collection interval than this stored value, the DCN throws an error and isn't able to fetch cluster performance data.

Solution

Work around this error by setting the collection interval to the same value for all vCenters:

1. Connect to the web client `https:// <vcenter server ip/hostname>`.
2. Select **vCenter Server**.
3. Select **Configure > General > Statistic**.
4. Click Edit.
5. Update the collection interval to equal the same value across your configured vCenters.
6. Save the configuration.

Virtual machine performance data is missing

Problem

Unable to get virtual machine performance data. This query doesn't return any results:

```
index="vmware-perf" source="VMPerf:VirtualMachine" | dedup sourcetype | table sourcetype
```

And on the Scheduler machine, you see the following error message in splunkd.log:

```
03-30-2020 13:34:04.693 +0100 ERROR ExecProcessor - message from "python
/opt/splunk/etc/apps/Splunk_TA_vmware/bin/ta_vmware_hierarchy_agent.py" splunk.AuthorizationFailed: [HTTP
403] Client is not authorized to perform requested action;
https://127.0.0.1:8089/servicesNS/nobody/Splunk_TA_vmware/storage/passwords/
```

Cause

The admin user has been renamed and Splunk no longer has an "admin" named user.

To collect virtual machine performance data, ta_vmware_hierarchy_agent.py scripted input prepares the list Virtual Machine moids. So if this list isn't created and shared with the data collection node (DCN), the DCN isn't able to collect performance data for them.

For this scripted input, the parameter "passAuth" is used for getting sessionKey for authentication purposes. It's value is admin, which means the 'admin' user is required to do the authentication.

Check `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/default/inputs.conf`

```
[script://$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin/ta_vmware_hierarchy_agent.py]
passAuth = admin
```

Resolution

There are 2 resolutions for this issue:

- On the scheduler machine, create a new user with the name "admin" and assign the "admin" and splunk_vmware_admin roles to admin user.
- Change the passAuth attribute value to the existing user name on the scheduler machine:

1. Add the `passAuth = splunk-system-user` parameter value to the following stanza in `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local/inputs.conf`:

   ```
   [script://$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin/ta_vmware_hierarchy_agent.py] passAuth =
   splunk-system-user
   ```
2. Restart Splunk.

No data collection when DCN is configured with more than 8 worker processes on Splunk version 8.x

Problem

When there are more than 8 worker processes configured, the scheduler throws the following error and data is not collected.

```
2020-09-30 15:06:50,550 ERROR [ta_vmware_collection_scheduler_inframon://Global pool] [HydraWorkerNode]
[establishGateway] could not connect to gateway=https://<DCN>:8008 for node=https://<DCN>:8089 due to a
socket error, timeout, or other fundamental communication issue, marking node as dead
```

Cause

In VMware add-on, the scheduler and the DCN communicate with each other through the hydra gateway server. When the add-on is installed on Splunk version 8.x and there are more than 8 worker processes configured for the DCNs, the hydra gateway server takes a longer time to respond to the request. The schedule isn't able to authenticate the hydra gateway server and no jobs are assigned to the DCNs.

Resolution

On the scheduler machine, go to the **Collection Configuration** page and edit the configured DCNs to update the worker process count to 8 or less. If more worker processes are required then configure new DCN machines. See Prepare to deploy the DCN for the standard guidelines.

Error for unexpected keyword argument 'rewrite' on Scheduler

Problem

When Splunkd is restarted, the DCNs stop collecting data and the scheduler for the Splunk Add-on for VMware throws the following error:

```
2020-09-21 19:25:01,199 ERROR [ta_vmware_collection_scheduler://puff] Problem with hydra scheduler
ta_vmware_collection_scheduler://puff:
 checkvCenterConnectivity() got an unexpected keyword argument 'rewrite'
 Traceback (most recent call last):
 File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 2126, in run
 self.checkvCenterConnectivity(rewrite=True)
 TypeError: checkvCenterConnectivity() got an unexpected keyword argument 'rewrite'
```

Cause

In the add-on, the "checkvCenterConnectivity" function is defined to check the connectivity of the configured vCenter server every 30 minutes.

Because this function is defined in the Splunk_TA_vmware package and is called from the SA-Hydra scheduler module, it requires a supported SA-Hydra version installed with the Splunk_TA_vmware package on the scheduler instance.

Resolution

Up grade SA-Hydra or Splunk_TA_vmware to versions that are compatible with each other. Also, make sure the scheduler, DCN, search, and indexer have the same add-on version.

Here's the version compatibility matrix for Splunk_TA_vmware and supported SA-Hydra:

Splunk_TA_vmware version	SA-Hydra version
3.4.4	4.0.8
3.4.5	4.0.9
3.4.6	4.1.0
3.4.7	4.1.1

Source types for the Splunk Add-on for VMware

The Splunk Add-on for VMware collects data from the following sources via:

- Modular input plus stdout
- Syslog
- File monitoring

For information about common information model configurations, see Common information model data model acceleration configurations.

Data source name	Source type	Event type	Collection method
VMInv:Datastore	vmware:inv:datastore	vmware_inventory	
		vmware_inv_datastore	
		vmware_perf_storage	
		vmware_performance	API
VMInv:VirtualMachine	vmware:inv:vm	vmware_inventory	
		vmware_inv_tools	
		vmware_inv_snapshot	
		vmware_inv_network	
		vmware_inv_storage	
		vmware_virtualmachine	API
VMInv:ClusterComputeResource	vmware:inv:clustercomputeresource		API
VMInv:ResourcePool	vmware:inv:resourcepool		API
VMInv:HostSystem	vmware:inv:hostsystem	vmware_inventory	
		vmware_inv_cpu	
		vmware_inv_mem	
		vmware_hostsystem	
		vmware_inv_os	API
VMInv:Hierarchy	vmware:inv:hierarchy		API
VMPerf:VirtualMachine	vmware:perf:sys	vmware_performance	
vmware_perf_os			
vmware_perf_uptime			
vmware_perf_time_sync		API	
VMPerf:VirtualMachine	vmware:perf:virtualDisk		API
VMPerf:VirtualMachine	vmware:perf:disk	vmware_perf_storage	API
VMPerf:VirtualMachine	vmware:perf:power		API
VMPerf:VirtualMachine	vmware:perf:mem	vmware_perf_mem	API

Data source name	Source type	Event type	Collection method
VMPerf:VirtualMachine	vmware:perf:rescpu		API
VMPerf:VirtualMachine	vmware:perf:cpu	vmware_perf_cpu	API
VMPerf:VirtualMachine	vmware:perf:datastore		API
VMPerf:VirtualMachine	vmware:perf:net	vmware_perf_network	API
VMPerf:HostSystem	vmware:perf:hbr		API
VMPerf:HostSystem	vmware:perf:disk	vmware_perf_storage	API
VMPerf:HostSystem	vmware:perf:datastore		API
VMPerf:HostSystem	vmware:perf:net	vmware_perf_network	API
VMPerf:HostSystem	vmware:perf:storageAdapter		API
VMPerf:HostSystem	vmware:perf:sys	vmware_performance	
		vmware_perf_os	
		vmware_perf_uptime	
		vmware_perf_time_sync	API
VMPerf:HostSystem	vmware:perf:rescpu		API
VMPerf:HostSystem	vmware:perf:power		API
VMPerf:HostSystem	vmware:perf:mem	vmware_perf_mem	API
VMPerf:HostSystem	vmware:perf:storagePath		API
VMPerf:HostSystem	vmware:perf:cpu	vmware_perf_cpu	API
VMPerf:HostSystem	vmware:perf:vflashModule		API
VMPerf:ClusterComputeResource	vmware:perf:cpu		
	vmware:perf:clusterServices		API
Username:XYZ	vmware:events	vmware_alert	API
Username:XYZ	vmware:tasks		API
.../vpxd.log	vmware:vclog:vpxd		File Monitoring
.../vpxd-profiler.log	vmware:vclog:vpxd-profiler		File Monitoring
.../vpxd-alert.log	vmware:vclog:vpxd-alert		File Monitoring
.../vmware/	vmware:vclog		File Monitoring
.../cim-diag,log	vmware:vclog:cim-diag		File Monitoring
vmware:esxilog:source::tcp:1514	vmware:esxlog:Hostd		File Monitoring
	vmware:esxlog:vmkernel		File Monitoring
	vmware:esxlog:Vpxa		File Monitoring
	vmware:esxlog:Fdm		File Monitoring
	vmware:esxlog:hostd-probe		File Monitoring
	vmware:esxlog:syslog		File Monitoring

	Source type	Event type	Collection method
Data source name	vmware:esxlog:crond		File Monitoring
	vmware:esxlog:smartd		File Monitoring
	vmware:esxlog:sfcb-CIMXML-Processor		File Monitoring
	vmware:esxilog:sfcb-vmware		File Monitoring
	vmware:esxlog:heartbeat		File Monitoring
	vmware:esxlog:vobd		File Monitoring
	vmware:esxlog:vmkwarning		File Monitoring
	vmware:esxlog:shell		File Monitoring
	vmware:esxlog:vmauthd		File Monitoring
	vmware:esxlog:sshd		File Monitoring
	vmware:esxlog:cimslp		File Monitoring
	vmware:esxlog:slpd		File Monitoring
	vmware:esxlog:ImageConfigManager		File Monitoring
	vmware:esxlog:Rhttpproxy		File Monitoring
	vmware:esxlog:storageRM		File Monitoring
	vmware:esxlog:root		File Monitoring
	vmware:esxlog:sfcb-hhrc		File Monitoring

Performance metrics reference

Use the performance metrics reference table to identify the metrics collected by the Splunk Add-on for VMware at the host and VM level. Learn what fields are present in VM events.

Entity	Field
hostsystem	p_average_cpu_coreUtilization_percent
hostsystem	p_average_cpu_demand_megaHertz
hostsystem	p_average_cpu_latency_percent
hostsystem	p_average_cpu_reservedCapacity_megaHertz
hostsystem	p_average_cpu_totalCapacity_megaHertz
hostsystem	p_average_cpu_usage_percent
hostsystem	p_average_cpu_usagemhz_megaHertz
hostsystem	p_average_cpu_utilization_percent
hostsystem	p_summation_cpu_costop_millisecond
hostsystem	p_summation_cpu_idle_millisecond
hostsystem	p_summation_cpu_ready_millisecond
hostsystem	p_summation_cpu_run_millisecond

Entity	Field
hostsystem	p_summation_cpu_swapwait_millisecond
hostsystem	p_summation_cpu_used_millisecond
hostsystem	p_summation_cpu_wait_millisecond
hostsystem	p_average_mem_active_kiloBytes
hostsystem	p_average_mem_activewrite_kiloBytes
hostsystem	p_average_mem_compressed_kiloBytes
hostsystem	p_average_mem_compressionRate_kiloBytesPerSecond
hostsystem	p_average_mem_consumed_kiloBytes
hostsystem	p_average_mem_decompressionRate_kiloBytesPerSecond
hostsystem	p_average_mem_granted_kiloBytes
hostsystem	p_average_mem_heap_kiloBytes
hostsystem	p_average_mem_heapfree_kiloBytes
hostsystem	p_average_mem_latency_percent
hostsystem	p_average_mem_llSwapIn_kiloBytes
hostsystem	p_average_mem_llSwapInRate_kiloBytesPerSecond
hostsystem	p_average_mem_llSwapOut_kiloBytes
hostsystem	p_average_mem_llSwapOutRate_kiloBytesPerSecond
hostsystem	p_average_mem_llSwapUsed_kiloBytes
hostsystem	p_average_mem_lowfreethreshold_kiloBytes
hostsystem	p_average_mem_overhead_kiloBytes
hostsystem	p_average_mem_reservedCapacity_megaBytes
hostsystem	p_average_mem_shared_kiloBytes
hostsystem	p_average_mem_sharedcommon_kiloBytes
hostsystem	p_average_mem_swapin_kiloBytes
hostsystem	p_average_mem_swapinRate_kiloBytesPerSecond
hostsystem	p_average_mem_swapout_kiloBytes
hostsystem	p_average_mem_swapoutRate_kiloBytesPerSecond
hostsystem	p_average_mem_swapused_kiloBytes
hostsystem	p_average_mem_sysUsage_kiloBytes
hostsystem	p_average_mem_totalCapacity_megaBytes
hostsystem	p_average_mem_unreserved_kiloBytes
hostsystem	p_average_mem_usage_percent
hostsystem	p_average_mem_vmmemctl_kiloBytes
hostsystem	p_average_mem_zero_kiloBytes

Entity	Field
hostsystem	p_latest_mem_state_number
hostsystem	p_average_disk_read_kiloBytesPerSecond
hostsystem	p_average_disk_usage_kiloBytesPerSecond
hostsystem	p_average_disk_write_kiloBytesPerSecond
hostsystem	p_latest_disk_maxTotalLatency_millisecond
hostsystem	p_latest_datastore_maxTotalLatency_millisecond
hostsystem	p_average_power_power_watt
hostsystem	p_average_power_powerCap_watt
hostsystem	p_summation_power_energy_joule
hostsystem	p_average_net_bytesRx_kiloBytesPerSecond
hostsystem	p_average_net_bytesTx_kiloBytesPerSecond
hostsystem	p_average_net_received_kiloBytesPerSecond
hostsystem	p_average_net_transmitted_kiloBytesPerSecond
hostsystem	p_average_net_usage_kiloBytesPerSecond
hostsystem	p_summation_net_broadcastRx_number
hostsystem	p_summation_net_broadcastTx_number
hostsystem	p_summation_net_droppedRx_number
hostsystem	p_summation_net_droppedTx_number
hostsystem	p_summation_net_errorsRx_number
hostsystem	p_summation_net_errorsTx_number
hostsystem	p_summation_net_multicastRx_number
hostsystem	p_summation_net_multicastTx_number
hostsystem	p_summation_net_packetsRx_number
hostsystem	p_summation_net_packetsTx_number
hostsystem	p_summation_net_unknownProtos_number
hostsystem	p_thruput
hostsystem	p_latest_rescpu_actav15_percent
hostsystem	p_latest_rescpu_actav1_percent
hostsystem	p_latest_rescpu_actav5_percent
hostsystem	p_latest_rescpu_actpk15_percent
hostsystem	p_latest_rescpu_actpk1_percent
hostsystem	p_latest_rescpu_actpk5_percent
hostsystem	p_latest_rescpu_maxLimited15_percent
hostsystem	p_latest_rescpu_maxLimited1_percent

Entity	Field
hostsystem	p_latest_rescpu_maxLimited5_percent
hostsystem	p_latest_rescpu_runav15_percent
hostsystem	p_latest_rescpu_runav1_percent
hostsystem	p_latest_rescpu_runav5_percent
hostsystem	p_latest_rescpu_runpk15_percent
hostsystem	p_latest_rescpu_runpk1_percent
hostsystem	p_latest_rescpu_runpk5_percent
hostsystem	p_latest_rescpu_sampleCount_number
hostsystem	p_latest_rescpu_samplePeriod_millisecond
hostsystem	p_average_hbr_hbrNetRx_kiloBytesPerSecond
hostsystem	p_average_hbr_hbrNetTx_kiloBytesPerSecond
hostsystem	p_average_hbr_hbrNumVms_number
hostsystem	p_latest_storageAdapter_maxTotalLatency_millisecond
hostsystem	p_latest_storagePath_maxTotalLatency_millisecond
hostsystem	p_latest_sys_uptime_second
hostsystem	p_uptime
virtualmachine	p_average_cpu_coreUtilization_percent
virtualmachine	p_average_cpu_demand_megaHertz
virtualmachine	p_average_cpu_latency_percent
virtualmachine	p_average_cpu_reservedCapacity_megaHertz
virtualmachine	p_average_cpu_totalCapacity_megaHertz
virtualmachine	p_average_cpu_usage_percent
virtualmachine	p_average_cpu_usagemhz_megaHertz
virtualmachine	p_average_cpu_utilization_percent
virtualmachine	p_latest_cpu_entitlement_megaHertz
virtualmachine	p_summation_cpu_costop_millisecond
virtualmachine	p_summation_cpu_idle_millisecond
virtualmachine	p_summation_cpu_maxlimited_millisecond
virtualmachine	p_summation_cpu_overlap_millisecond
virtualmachine	p_summation_cpu_ready_millisecond
virtualmachine	p_summation_cpu_run_millisecond
virtualmachine	p_summation_cpu_system_millisecond
virtualmachine	p_summation_cpu_swapwait_millisecond
virtualmachine	p_summation_cpu_used_millisecond

Entity	Field
virtualmachine	p_summation_cpu_wait_millisecond
virtualmachine	p_average_mem_active_kiloBytes
virtualmachine	p_average_mem_activewrite_kiloBytes
virtualmachine	p_average_mem_compressed_kiloBytes
virtualmachine	p_average_mem_compressionRate_kiloBytesPerSecond
virtualmachine	p_average_mem_consumed_kiloBytes
virtualmachine	p_average_mem_decompressionRate_kiloBytesPerSecond
virtualmachine	p_average_mem_entitlement_kiloBytes
virtualmachine	p_average_mem_granted_kiloBytes
virtualmachine	p_average_mem_heap_kiloBytes
virtualmachine	p_average_mem_heapfree_kiloBytes
virtualmachine	p_average_mem_latency_percent
virtualmachine	p_average_mem_llSwapIn_kiloBytes
virtualmachine	p_average_mem_llSwapInRate_kiloBytesPerSecond
virtualmachine	p_average_mem_llSwapOut_kiloBytes
virtualmachine	p_average_mem_llSwapOutRate_kiloBytesPerSecond
virtualmachine	p_average_mem_llSwapUsed_kiloBytes
virtualmachine	p_average_mem_lowfreethreshold_kiloBytes
virtualmachine	p_average_mem_overhead_kiloBytes
virtualmachine	p_average_mem_overheadMax_kiloBytes
virtualmachine	p_average_mem_overheadTouched_kiloBytes
virtualmachine	p_average_mem_reservedCapacity_megaBytes
virtualmachine	p_average_mem_shared_kiloBytes
virtualmachine	p_average_mem_sharedcommon_kiloBytes
virtualmachine	p_average_mem_swapin_kiloBytes
virtualmachine	p_average_mem_swapinRate_kiloBytesPerSecond
virtualmachine	p_average_mem_swapout_kiloBytes
virtualmachine	p_average_mem_swapoutRate_kiloBytesPerSecond
virtualmachine	p_average_mem_swapped_kiloBytes
virtualmachine	p_average_mem_swaptarget_kiloBytes
virtualmachine	p_average_mem_swapused_kiloBytes
virtualmachine	p_average_mem_sysUsage_kiloBytes
virtualmachine	p_average_mem_totalCapacity_megaBytes
virtualmachine	p_average_mem_unreserved_kiloBytes

Entity	Field
virtualmachine	p_average_mem_usage_percent
virtualmachine	p_average_mem_vmmemctl_kiloBytes
virtualmachine	p_average_mem_vmmemctltarget_kiloBytes
virtualmachine	p_average_mem_zero_kiloBytes
virtualmachine	p_latest_mem_state_number
virtualmachine	p_latest_mem_zipped_kiloBytes
virtualmachine	p_latest_mem_zipSaved_kiloBytes
virtualmachine	p_average_disk_read_kiloBytesPerSecond
virtualmachine	p_average_disk_usage_kiloBytesPerSecond
virtualmachine	p_average_disk_write_kiloBytesPerSecond
virtualmachine	p_latest_disk_maxTotalLatency_millisecond
virtualmachine	p_latest_datastore_maxTotalLatency_millisecond
virtualmachine	p_average_power_power_watt
virtualmachine	p_average_power_powerCap_watt
virtualmachine	p_summation_power_energy_joule
virtualmachine	p_average_net_bytesRx_kiloBytesPerSecond
virtualmachine	p_average_net_bytesTx_kiloBytesPerSecond
virtualmachine	p_average_net_received_kiloBytesPerSecond
virtualmachine	p_average_net_transmitted_kiloBytesPerSecond
virtualmachine	p_average_net_usage_kiloBytesPerSecond
virtualmachine	p_summation_net_broadcastRx_number
virtualmachine	p_summation_net_broadcastTx_number
virtualmachine	p_summation_net_droppedRx_number
virtualmachine	p_summation_net_droppedTx_number
virtualmachine	p_summation_net_errorsRx_number
virtualmachine	p_summation_net_errorsTx_number
virtualmachine	p_summation_net_multicastRx_number
virtualmachine	p_summation_net_multicastTx_number
virtualmachine	p_summation_net_packetsRx_number
virtualmachine	p_summation_net_packetsTx_number
virtualmachine	p_summation_net_unknownProtos_number
virtualmachine	p_thruput
virtualmachine	p_latest_rescpu_actav15_percent
virtualmachine	p_latest_rescpu_actav1_percent

Entity	Field
virtualmachine	p_latest_rescpu_actav5_percent
virtualmachine	p_latest_rescpu_actpk15_percent
virtualmachine	p_latest_rescpu_actpk1_percent
virtualmachine	p_latest_rescpu_actpk5_percent
virtualmachine	p_latest_rescpu_maxLimited15_percent
virtualmachine	p_latest_rescpu_maxLimited1_percent
virtualmachine	p_latest_rescpu_maxLimited5_percent
virtualmachine	p_latest_rescpu_runav15_percent
virtualmachine	p_latest_rescpu_runav1_percent
virtualmachine	p_latest_rescpu_runav5_percent
virtualmachine	p_latest_rescpu_runpk15_percent
virtualmachine	p_latest_rescpu_runpk1_percent
virtualmachine	p_latest_rescpu_runpk5_percent
virtualmachine	p_latest_rescpu_sampleCount_number
virtualmachine	p_latest_rescpu_samplePeriod_millisecond
virtualmachine	p_latest_sys_osUptime_second
virtualmachine	p_latest_sys_uptime_second
virtualmachine	p_summation_sys_heartbeat_number
virtualmachine	p_uptime

See the VMware Technology Network documentation for more information

- vCenter Performance Counters table on VMware Technology Network.
- Performance metrics in the *Performance and VMmark* section of the VMware Technology Network.

See the *Working with Statistics* section of the VMware vSphere ESX and vCenter documentation to find information

- Statistics Collection for vCenter Server
- Statistics Collection for Microsoft Windows Guest Operating Systems
- vCenter Server Performance Charts
- Monitoring and Troubleshooting performance

See the VMWare developer support page for information

- Counters for Disk Performance
- Counters for Memory Performance
- Counters for CPU Performance
- Managed object performance manager

Data collection configuration file reference

Edit `ta_vmware_collection.conf` on the scheduler to enable or disable instance level data and to allow or deny metric collection. You can find the specification for `ta_vmware_collection.conf` in `Splunk_TA_vmware/bin/ta_vmware/models.py`.

```
  # Copyright (C) 2005-2021 Splunk Inc. All Rights Reserved.

[default]
#These are all the tasks that should run everywhere
task = hostvmperf, otherperf, hierarchyinv, hostinv, vminv, clusterinv, datastoreinv, rpinv, task, event
#These are the tasks that should be considered atomic and not generate jobs until the previous run completes
atomic_tasks = hostinv, vminv
#atomic task confirmation expirations automatically unlock jobs after the elapsed time even if a completion
or failure has not been logged. The defaults are double interval.
#hostinv_confirmation_expiration = 1800
#vminv_confirmation_expiration = 1800

#These are the destination indexes for the different data types
perf_index = vmware-perf
inv_index = vmware-inv
taskevent_index = vmware-taskevent
# Object count value in API response for inventory collector
# This values has to be greater than equal to 1. If you set this value with higher value then hostinv will
take more memory
# to process the api response. If you set this value too low then it increases the load on VC as API calls
increase.
#inv_maxObjUpdates = 20
#The following are the collection intervals for particular tasks
hostvmperf_interval = 180
# Setting interval to < 30 min results in missing cluster data
otherperf_interval = 2000
hierarchyinv_interval = 300
hostinv_interval = 900
vminv_interval = 900
clusterinv_interval = 1800
datastoreinv_interval = 900
rpinv_interval = 900
task_interval = 300
event_interval = 300
#The following are the expiration periods for particular tasks
hostvmperf_expiration = 180
otherperf_expiration = 1900
task_expiration = 3600
event_expiration = 3600
hierarchyinv_expiration = 300
hostinv_expiration = 900
vminv_expiration = 900
clusterinv_expiration = 1800
datastoreinv_expiration = 900
rpinv_expiration = 900

# The number to add to the priority number for jobs of a given task, negative number makes higher priority
task_priority = -60
event_priority = -60
hierarchyinv_priority = -120

#Performance format type. This is used to define format which is used to retrieve perf data form vmware.
Make sure it has value either csv or normal
perf_format_type = csv
```

```
# For HostSystem Inv, only config.hyperThread is collected by default
# Add other properties as follows, example:
# hostsystem_inv_config = config.adminDisabled, config.host
# Default allowlists / denylists for entities:
# resource pools should be turned off
perf_entity_denylist = ^ResourcePool$
# Default allowlists / denylists for metrics:
# for clusters, only clusterServices counter group should be collected
cluster_metric_allowlist = ^p_(?!average_cpu_reservedCapacity_megaHertz).*_(clusterServices|cpu).*
# adding on demand aggregated metrics as denylist
cluster_metric_denylist =
^p_((maximum|minimum)_(cpu_usagemhz_megaHertz|cpu_usage_percent)|average_cpu_corecount.contention_percent)
# datagen flags for internal use only
autoeventgen = false
autoeventgen_poweroff_vmcount = 0

# The following lines should NOT be commented if you want to collect instance level data
# host_instance_allowlist = .*
# vm_instance_allowlist = .*
# rp_instance_allowlist = .*
# cluster_instance_allowlist = .*

deployment_type = VMware
```

Data model acceleration configuration file reference

Edit datamodels.conf, located on your search head at: `/etc/apps/`

The default configurations of the Data Model properties are:

SA-VMW-HierarchyInventory/default/datamodels.conf

```
[VMwareInventory]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.cron_schedule = */5 * * * *
```

SA-VMW-Performance/default/datamodels.conf

```
[VMwarePerformance]
acceleration = 1
acceleration.earliest_time = -1mon
acceleration.cron_schedule = */5 * * * *
```

Splunk Add-on for Netapp Data ONTAP

See the Splunk Add-on for NetApp Data ONTAP installation section to receive NetApp Data ONTAP data on your Splunk platform deployment.

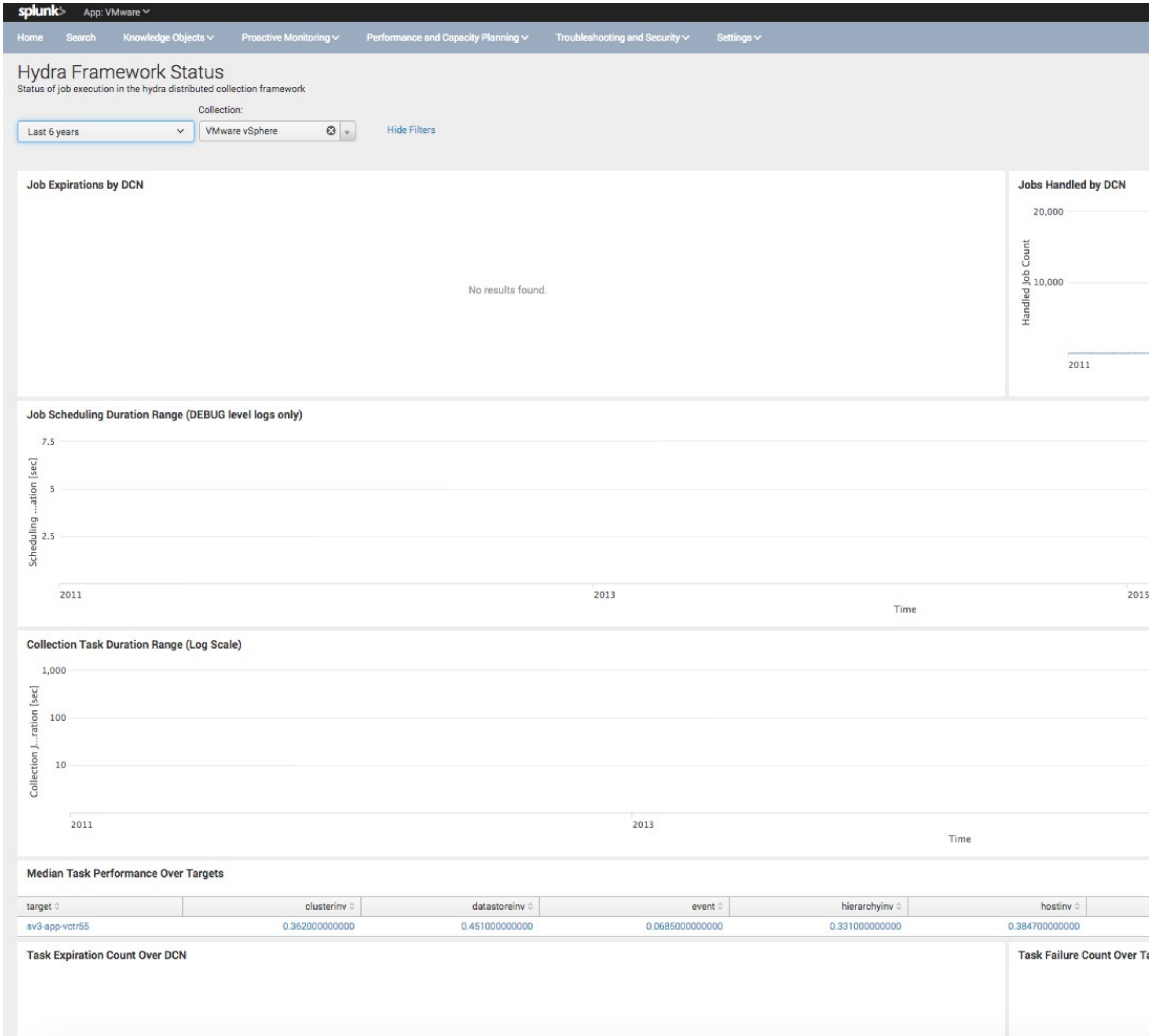
Hydra Framework Status

Use the Hydra Framework Status page to identify issues related to jobs handled by **SA-Hydra**. To view the Hydra Framework Status page, select the Hydra Framework Status page from the Splunk Add-on for VMware dropdown menu to view the page or open **Dashboards** from Search & Reporting App.

Enable data population for this page.

1. Navigate to `Splunk_TA_vmware/local/input.conf`
2. Set the `log_level` to `DEBUG` for all enabled worker stanzas.
3. Save your changes and restart your Splunk platform deployment.

Dashboard name	Description
Job Expirations by DCN	Number of jobs assigned and expired on each DCN versus time. DCN (Worker) logs are required to populate this panel.
Jobs Handled by DCN	Number of jobs successfully completed by each DCN versus time. DCN (Worker) logs are required to populate this panel.
Job Scheduling Duration Range (DEBUG level logs only)	Average, Max and Min time taken for Scheduler to assign jobs to DCNs at every iteration versus time. It will populate when DEBUG level is enabled on your scheduler. Scheduler logs are required to populate this panel.
Collection Task Duration Range (Log Scale)	Minimum, Median and Maximum execution time to perform all the task. DCN (Worker) logs are required to populate this panel.
Median Task Performance Over Targets	Target (vCenter) and task wise median job execution time reported by Worker on DCN. DCN (Worker) logs are required to populate this panel.
Task Expiration Count Over DCN	Task wise no. of jobs assigned and expired on each DCN. DCN (Worker) logs are required to populate this panel.
Task Failure Count Over Target	Task wise no. of jobs assigned and failed on each DCN. DCN (Worker) logs are required to populate this panel.
Last 100 Worker Errors - excluding expiration	Last 100 errors occurred in worker processes in all DCNs excluding errors which occurred due to job expiration. DCN (Worker) logs are required to populate this panel.
Last 100 Scheduler Errors	Last 100 errors occurred in Scheduler process. Scheduler logs are required to populate this panel.



Hydra Framework Status

Status of job execution in the hydra distributed collection framework

Last 6 years

Collection: VMware vSphere

Job Expirations by DCN

No results found.

Jobs Handled by DCN

Job Scheduling Duration Range (DEBUG level logs only)

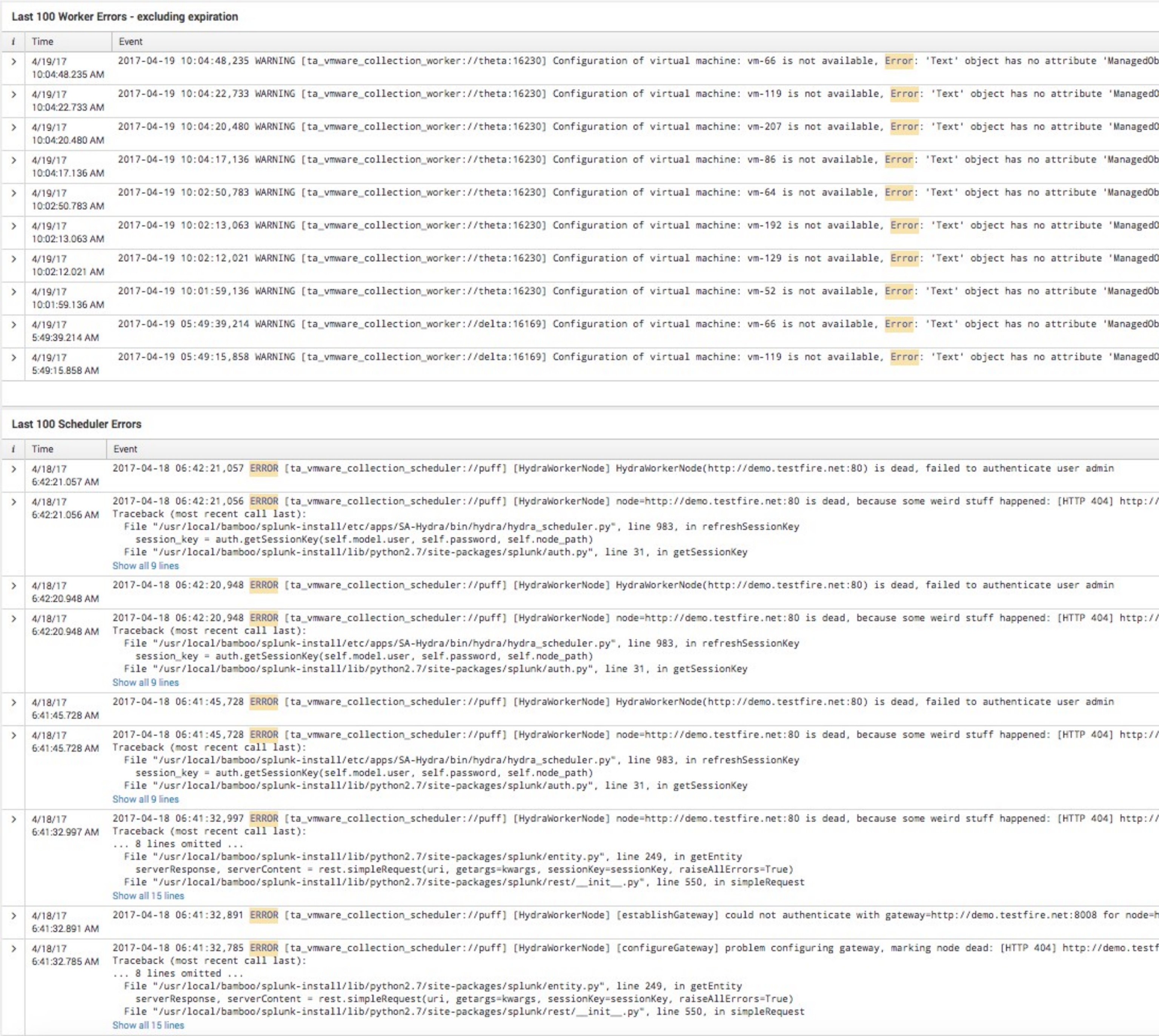
Collection Task Duration Range (Log Scale)

Median Task Performance Over Targets

target	clusterinv	datastoreinv	event	hierarchyinv	hostinv
sv3-app-vctr55	0.362000000000	0.451000000000	0.0685000000000	0.331000000000	0.384700000000

Task Expiration Count Over DCN

Task Failure Count Over Ta



Last 100 Worker Errors - excluding expiration

```
i  Time              Event
>  4/19/17           2017-04-19 10:04:48,235 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-66 is not available, Error: 'Text' object has no attribute 'ManagedOb
   10:04:48.235 AM
>  4/19/17           2017-04-19 10:04:22,733 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-119 is not available, Error: 'Text' object has no attribute 'ManagedO
   10:04:22.733 AM
>  4/19/17           2017-04-19 10:04:20,480 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-207 is not available, Error: 'Text' object has no attribute 'ManagedO
   10:04:20.480 AM
>  4/19/17           2017-04-19 10:04:17,136 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-86 is not available, Error: 'Text' object has no attribute 'ManagedOb
   10:04:17.136 AM
>  4/19/17           2017-04-19 10:02:50,783 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-64 is not available, Error: 'Text' object has no attribute 'ManagedOb
   10:02:50.783 AM
>  4/19/17           2017-04-19 10:02:13,063 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-192 is not available, Error: 'Text' object has no attribute 'ManagedO
   10:02:13.063 AM
>  4/19/17           2017-04-19 10:02:12,021 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-129 is not available, Error: 'Text' object has no attribute 'ManagedO
   10:02:12.021 AM
>  4/19/17           2017-04-19 10:01:59,136 WARNING [ta_vmware_collection_worker://theta:16230] Configuration of virtual machine: vm-52 is not available, Error: 'Text' object has no attribute 'ManagedOb
   10:01:59.136 AM
>  4/19/17           2017-04-19 05:49:39,214 WARNING [ta_vmware_collection_worker://delta:16169] Configuration of virtual machine: vm-66 is not available, Error: 'Text' object has no attribute 'ManagedOb
   5:49:39.214 AM
>  4/19/17           2017-04-19 05:49:15,858 WARNING [ta_vmware_collection_worker://delta:16169] Configuration of virtual machine: vm-119 is not available, Error: 'Text' object has no attribute 'ManagedO
   5:49:15.858 AM
```

Last 100 Scheduler Errors

```
i  Time             Event
>  4/18/17          2017-04-18 06:42:21,057 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] HydraWorkerNode(http://demo.testfire.net:80) is dead, failed to authenticate user admin
   6:42:21.057 AM
>  4/18/17          2017-04-18 06:42:21,056 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] node=http://demo.testfire.net:80 is dead, because some weird stuff happened: [HTTP 404] http://
   6:42:21.056 AM   Traceback (most recent call last):
                      File "/usr/local/bamboo/splunk-install/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 983, in refreshSessionKey
                        session_key = auth.getSessionKey(self.model.user, self.password, self.node_path)
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/auth.py", line 31, in getSessionKey
                    Show all 9 lines
>  4/18/17          2017-04-18 06:42:20,948 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] HydraWorkerNode(http://demo.testfire.net:80) is dead, failed to authenticate user admin
   6:42:20.948 AM
>  4/18/17          2017-04-18 06:42:20,948 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] node=http://demo.testfire.net:80 is dead, because some weird stuff happened: [HTTP 404] http://
   6:42:20.948 AM   Traceback (most recent call last):
                      File "/usr/local/bamboo/splunk-install/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 983, in refreshSessionKey
                        session_key = auth.getSessionKey(self.model.user, self.password, self.node_path)
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/auth.py", line 31, in getSessionKey
                    Show all 9 lines
>  4/18/17          2017-04-18 06:41:45,728 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] HydraWorkerNode(http://demo.testfire.net:80) is dead, failed to authenticate user admin
   6:41:45.728 AM
>  4/18/17          2017-04-18 06:41:45,728 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] node=http://demo.testfire.net:80 is dead, because some weird stuff happened: [HTTP 404] http://
   6:41:45.728 AM   Traceback (most recent call last):
                      File "/usr/local/bamboo/splunk-install/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 983, in refreshSessionKey
                        session_key = auth.getSessionKey(self.model.user, self.password, self.node_path)
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/auth.py", line 31, in getSessionKey
                    Show all 9 lines
>  4/18/17          2017-04-18 06:41:32,997 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] node=http://demo.testfire.net:80 is dead, because some weird stuff happened: [HTTP 404] http://
   6:41:32.997 AM   Traceback (most recent call last):
                    ... 8 lines omitted ...
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/entity.py", line 249, in getEntity
                        serverResponse, serverContent = rest.simpleRequest(uri, getargs=kwargs, sessionKey=sessionKey, raiseAllErrors=True)
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/rest/__init__.py", line 550, in simpleRequest
                    Show all 15 lines
>  4/18/17          2017-04-18 06:41:32,891 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] [establishGateway] could not authenticate with gateway=http://demo.testfire.net:8008 for node=h
   6:41:32.891 AM
>  4/18/17          2017-04-18 06:41:32,785 ERROR [ta_vmware_collection_scheduler://puff] [HydraWorkerNode] [configureGateway] problem configuring gateway, marking node dead: [HTTP 404] http://demo.testf
   6:41:32.785 AM   Traceback (most recent call last):
                    ... 8 lines omitted ...
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/entity.py", line 249, in getEntity
                        serverResponse, serverContent = rest.simpleRequest(uri, getargs=kwargs, sessionKey=sessionKey, raiseAllErrors=True)
                      File "/usr/local/bamboo/splunk-install/lib/python2.7/site-packages/splunk/rest/__init__.py", line 550, in simpleRequest
                    Show all 15 lines
```

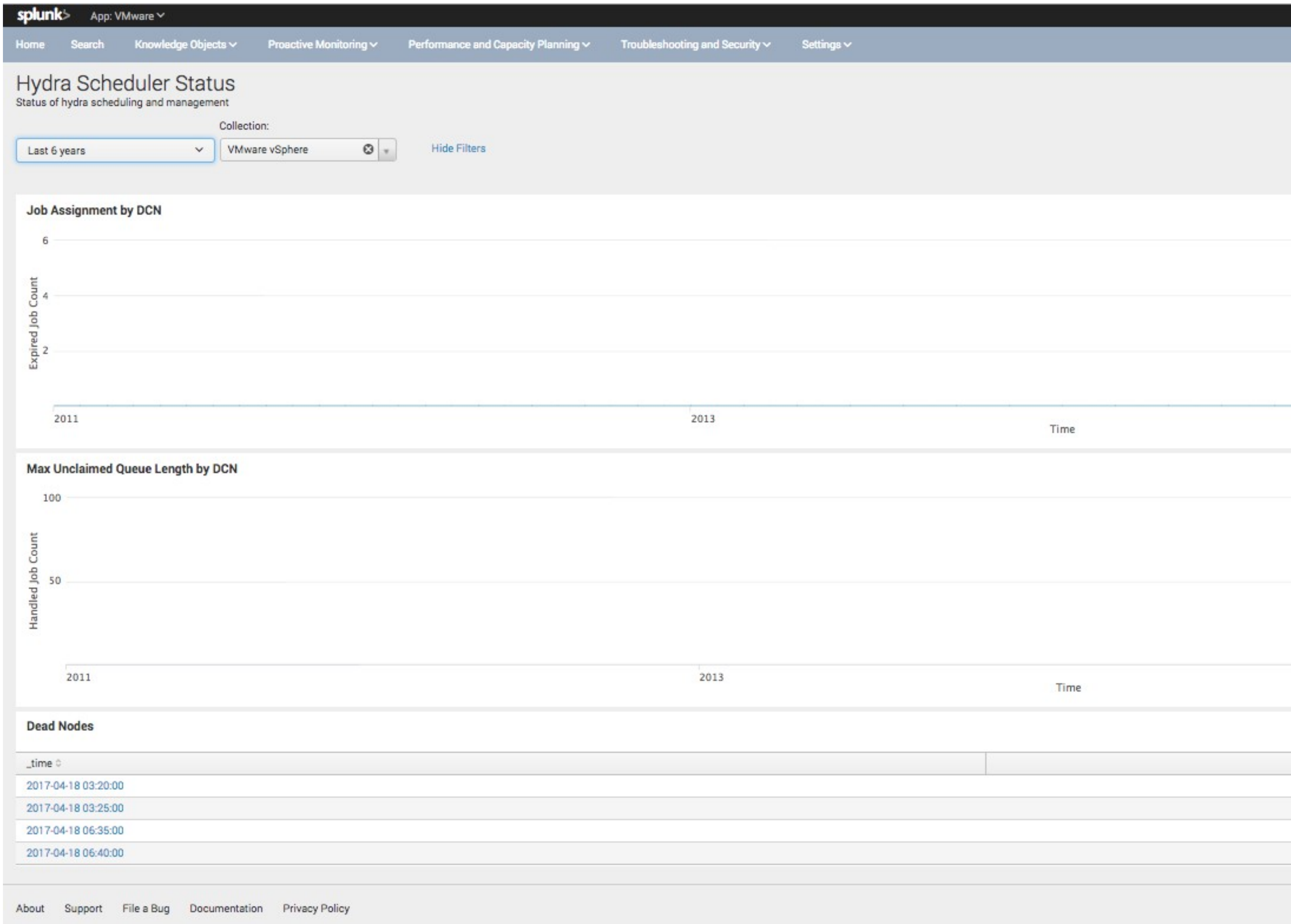
Hydra Scheduler Status

Use the Hydra Scheduler Status page to identify issues related to jobs handled your scheduler. To view the Hydra Scheduler Status page, select the Hydra Scheduler Status page from the Splunk Add-on for VMware dropdown menu to view the page or open **Dashboards** from Search & Reporting App.

Enable data population for this page.

1. Navigate to `Splunk_TA_vmware/local/input.conf`
2. Set the `log_level` to `DEBUG` for all enabled worker stanzas.
3. Save your changes and restart your Splunk platform deployment.

Dashboard name	Description
Job Assignment by DCN	Number of jobs assigned to each DCN versus time. It will populate when DEBUG level is enabled on scheduler. Scheduler logs are required to populate this panel.
Max Unclaimed Queue Length by DCN	Number of unclaimed jobs reported by each DCN to Scheduler versus time. It will populate when DEBUG level is enabled on scheduler. Scheduler logs are required to populate this panel.
Dead Nodes	List of dead nodes (DCNs) and their count at every 5 minute interval. Scheduler logs are required to populate this panel.



Hydra Scheduler Status

Status of hydra scheduling and management

Last 6 years

Collection: VMware vSphere

Job Assignment by DCN

Max Unclaimed Queue Length by DCN

Dead Nodes

_time
2017-04-18 03:20:00
2017-04-18 03:25:00
2017-04-18 06:35:00
2017-04-18 06:40:00

Third-Party Software

Credits

Some of the components included in Splunk Add-on for VMware are licensed under free or open-source licenses. We wish to thank the contributors to those projects.

View the license(s) associated with each component by selecting a component name on the left.

Suds (Python 2)

Suds version 0.4.1

https://pypi.python.org/pypi/suds

This program is free software; you can redistribute it and/or modify it under the terms of the (LGPL) GNU Lesser General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library Lesser General Public License for more details at (http://www.gnu.org/licenses/lgpl.html).

You should have received a copy of the GNU Lesser General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. written by: Jeff Ortel

(jortel@redhat.com)

Suds (Python 3)

suds (Python 3) Version 1.3.3.0

https://pypi.org/project/suds-py3/

This program is free software; you can redistribute it and/or modify it under the terms of the (LGPL) GNU Lesser General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library Lesser General Public License for more details at http://www.gnu.org/licenses/lgpl.html.

You should have received a copy of the GNU Lesser General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Written by: Jeff Ortel (jortel@redhat.com)

Axios

https://github.com/axios/axios

Version 0.19.2

Copyright (c) 2014-present Matt Zabriskie

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Suds (Python 2)

https://pypi.python.org/pypi/suds

Suds version 0.4.1

This program is free software; you can redistribute it and/or modify it under the terms of the (LGPL) GNU Lesser General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library Lesser General Public License for more details at (http://www.gnu.org/licenses/lgpl.html).

You should have received a copy of the GNU Lesser General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. written by: Jeff Ortel

(jortel@redhat.com)