Splunk® Supported Add-ons
Splunk Add-on for vCenter Logs released

Generated: 11/05/2022 12:01 pm

Table of Contents

Overview

About the Splunk Add-on for vCenter Logs

Version	4.2.1
Vendor products	VMware vCenter Server versions 6.5, 6.7, 7.0

Splunk Add-on for vCenter logs contains the input stanzas to receive the data from the syslog, monitoring input stanzas to monitor vCenter log data from your vCenter environment, and search-time and index-time extractions to parse and extract the fields from the vCenter logs. The Splunk Add-on for vCenter Logs collects vCenter log data and forwards it to the indexers in your environment.

The package included in Splunk Add-on for vCenter Logs (Splunk_TA_vcenter) was previously part of Splunk Add-on for VMware Metrics in v4.2.0 or below and the Splunk Add-on for VMware in v4.0.2 or below. This package is published as the Splunk Add-on for vCenter Logs, an individual Splunkbase add-on, to add support for self-service installation in cloud environments for the Splunk Add-on for VMware Metrics v4.2.1 or the Splunk Add-on for VMware v4.0.3.

Download the Splunk Add-on for vCenter Logs from Splunkbase at https://splunkbase.splunk.com/app/5601.

Release notes for the Splunk Add-on for VMware vCenter Logs

Version 4.2.1 of the Splunk Add-on for VMware vCenter Logs was released on June 28, 2021. This is the first release of Splunk Add-on for VMware vCenter Logs.

The package included in Splunk Add-on for VMware vCenter logs (Splunk_TA_vcenter) was previously part of Splunk Add-on for VMware Metrics in v4.2.0 or previous and Splunk Add-on for VMware in v4.0.2 or previous. This package is being released as an individual Splunkbase add-on to add support for self-service installation for the Splunk Add-on for VMware Metrics or the Splunk Add-on for VMware in cloud environments.

What's new

These features are available in the Splunk Add-on for VMware vCenter logs v4.2.1. For compatibility information, go to the Data collection planning and requirements.

New feature or enhancement	Description
Ingestion and Parsing of VMware vCenter log data	The package contains the input stanzas to receive the data from the syslog, the monitoring input stanzas to monitor data from your vCenter environment, and the search-time and index-time extractions to parse and extract the fields from the vCenter logs.
Support for self-service installation in cloud environments	Customers of the Splunk Add-on for VMware Metrics or Splunk Add-on for VMware on cloud environment can install this package by following the cloud installation steps. As the add-on package was previously part of the Splunk Add-on for VMware Metrics v4.2.0 or previous and Splunk Add-on for VMware in v4.0.2 or previous, existing customers of Splunk

New feature or enhancement	Description
	Add-on for VMware Metrics have to follow the upgrade steps for the Splunk Add-on for VMware Metrics to switch to the version of the add-on that supports the self-service installation. Existing customers of the Splunk Add-on for VMware have to follow the upgrade steps for the Splunk Add-on for VMware to switch to the version of the add-on that supports self-service installation

Fixed issues

This version of the Splunk Add-on for VMware vCenter Logs 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 vCenter Logs 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.
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.
2020-06-22	VMW-5473	After upgrade to Splunk add on for VMware Metrics 4.x vCenter/DCN configuration showing wrong "last connected time"
2020-06-01	VMW-5425	There's an invalid key error on Splunk version 7.x because Splunk Add-on for VMware Metrics uses the Python 3 interpreter by default.
2019-10-15	VMW-5274	For inventory data, the changeset field value is null.
2019-08-22	VMW-5188	There can be irregular collection intervals and negative values for performance metrics.
2019-06-12	VMW-5127	There can be duplicate performance metrics data.
2019-06-06	VMW-5118	The Cluster performance value is incorrect for metrics due to the aggregation mechanism on the vCenter side.
2018-04-25	VMW-4848	DCN collection worker failures - vmodl.query.PropertyCollector:session exceptions.

Release History for the Splunk Add-on for vCenter Logs

Latest release

The latest version of the Splunk Add-on for vCenterLogs is 4.2.1. Go to Release notes for the Splunk Add-on for vCenter Logs for the release notes of this latest version.

Installation and Configuration

Data collection planning and requirements for the Splunk Add-on for vCenter Logs

Before you deploy the Splunk Add-on for vCenter Logs review these requirements.

Splunk platform version requirements

- For Splunk Enterprise system requirements, go to System requirements for use of Splunk Enterprise on-premises in the Splunk Enterprise Installation Manual.
- For Splunk Light system requirements, go to System Requirements in the Splunk Light in the Splunk Light Installation Manual.
- If you're managing on-premises forwarders to get data into Splunk Cloud, go to System requirements for use of Splunk Enterprise on-premises, which includes information about forwarders.

Current add-on version	Supported versions of Splunk Enterprise
4.2.1	• 8.0.x • 8.1.x • 8.2.x • 9.0.0

VMware index

The vCenter logs data forwarded from the forwarder is stored in this index. The Splunk Add-on for vCenter Logs package indexes the data into the vmware-vclog index defined in Splunk Add-on for VMware Metrics Indexes. If you are using Splunk Add-on for VMware Metrics, then you need to install Splunk Add-on for VMware Metrics Indexes in your environment to get this index. If you are using Splunk Add-on for VMware, then you need to install Splunk Add-on for VMware Indexes in your environment to get the index."

Index	Description
vmware-vclog	Stores vCenter server log data.

Data volume requirements

The expected vCenter logs data volume ingested by this package in a typical environment is 15 MB per host per day. The actual volume varies depending on the log data collected and the number of virtual machines on a host.

Data type	Data volumne
vCenter server logs	15 MB per host per day

Add-on Version compatibility with Splunk Add-on for VMware Metrics and its prerequisite add-ons

Splunk Add-on for VMware Metrics version	Compatible Splunk Add-on for vCenter Logs version	Compatible Splunk Add-on for VMware Metrics Indexes version	Compatible vCenter version	Compatible ESXi version
4.2.1	4.2.1	4.2.1	• 6.5 • 6.7 • 7.0	• 6.5 • 6.7 • 7.0

Add-on Version compatibility with Splunk Add-on for VMware and its prerequisite add-ons

Splunk Add-on for VMware version	Compatible Splunk Add-on for vCenter Logs version	Compatible Splunk Add-on for VMware Indexes version	Compatible vCenter version	Compatible ESXi version
4.0.3	4.2.1	4.0.3	• 6.5 • 6.7 • 7.0	• 6.5 • 6.7 • 7.0
4.0.4	4.2.1	4.0.3	• 6.5 • 6.7 • 7.0	• 6.5 • 6.7 • 7.0

Installation and configuration overview for the Splunk Add-on for vCenter Logs

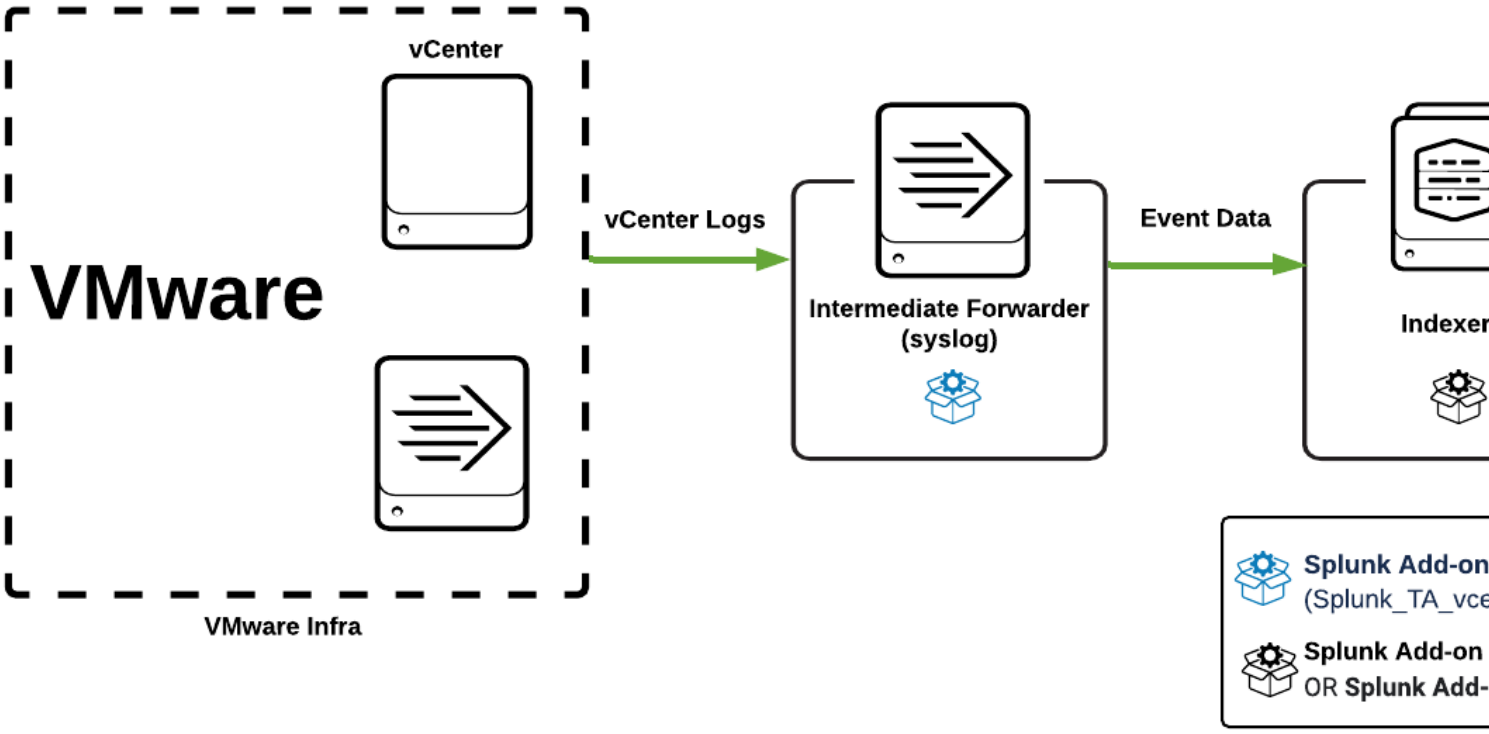
The Splunk Add-on for vCenter logs package contains necessary Index-time and search-time extractions to parse the vCenter logs collected using the syslog/forwarder installed on vCenter server. This overview outlines a full installation of the Splunk Add-on for vCenter Logs on a distributed deployment.

Install the Splunk Add-on for vCenter Logs

Review the deployment diagram and corresponding table for your environment type for details on the install locations for each vCenter logs data collection package. If you are using an on-premises environment, you can forward the data directly to the indexer or using an intermediate forwarder (such as DCN). If you are using the add-on in a cloud environment, you have to forward the data to an intermediate heavy forwarder before you forward the data to cloud indexers.

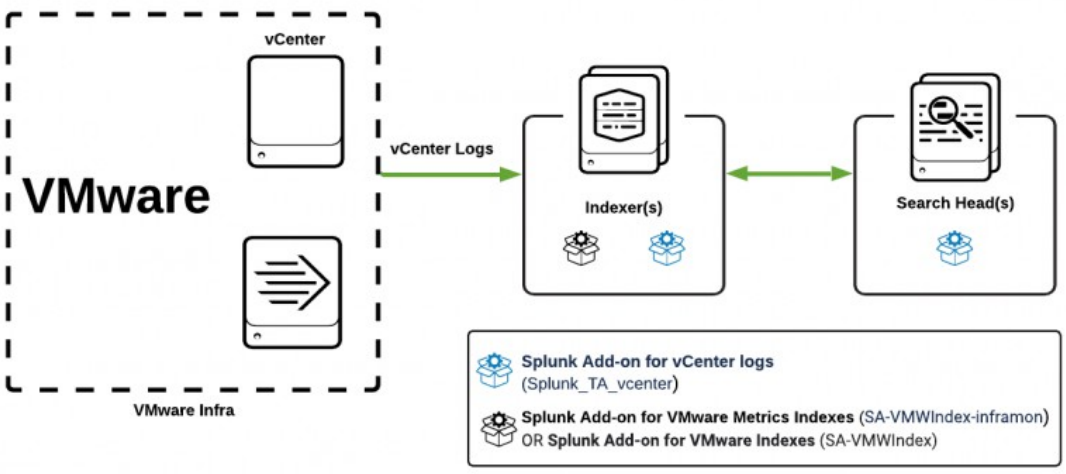
Install Splunk Add-on for vCenter Logs in an on-premises environment

This deployment diagram reflects the best practice for deploying the Splunk Add-on for vCenter Logs in an on-premises environment.


vCenter
VMware
VMware Infra
vCenter Logs
Intermediate Forwarder
(syslog)
Event Data
Indexer
Splunk Add-on
(Splunk_TA_vce
Splunk Add-on
OR Splunk Add-

This deployment diagram and corresponding table outline the full installation of Splunk Add-on for vCenter Logs in an on-premises environment.

This deployment diagram and the corresponding table represent an alternative option for deploying the Splunk Add-on for vCenter Logs in an on-premises environment.



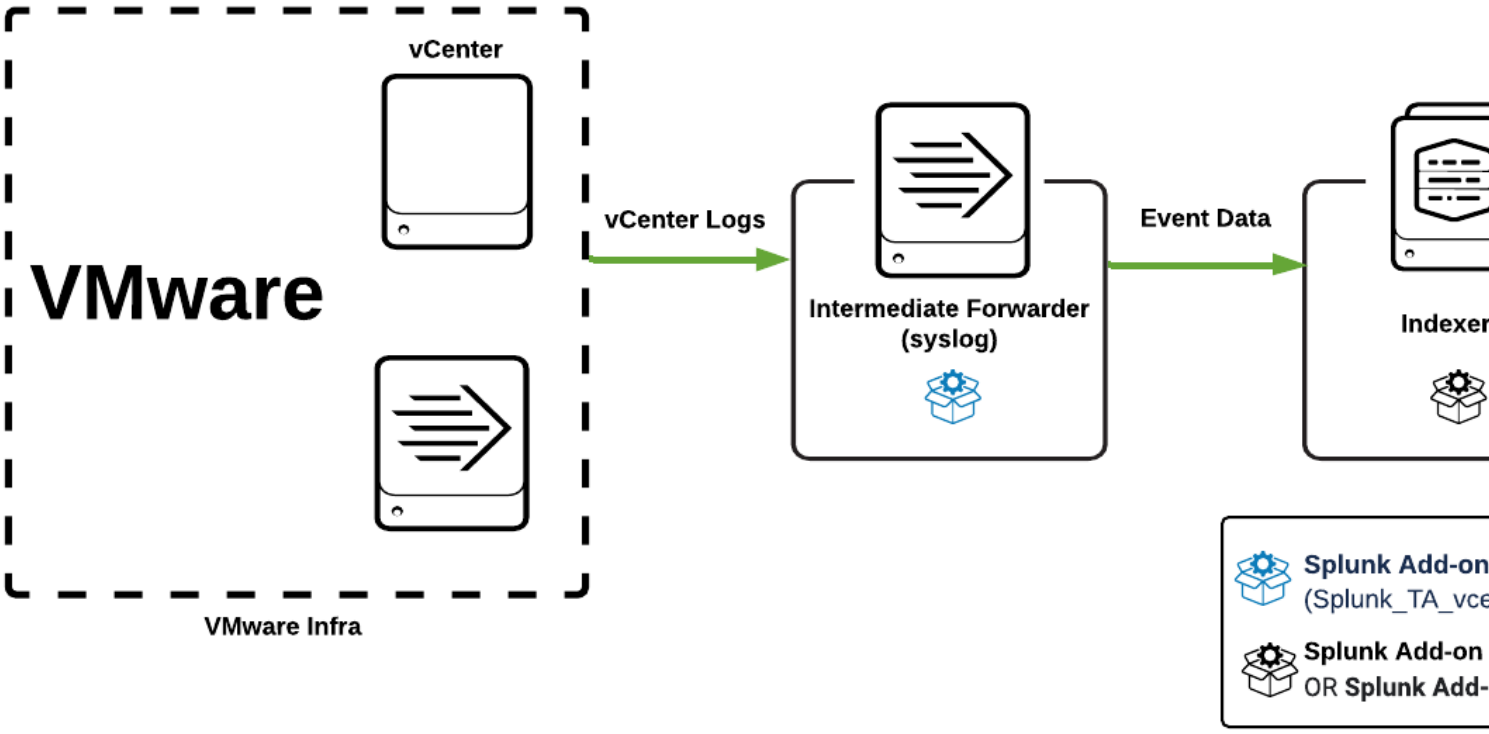
Add-on	Package	Search head	Indexer	Data collection node (DCN)	Dedicated vCenter log forwarder	The operation performed by the pacakage
Splunk Add-on for vCenter Logs	Splunk_TA_vcenter	X	X*	X†	X	Handles log data collection and parsing of vCenter logs.
Splunk Add-on for VMware Metrics Indexes or Splunk Add-on for VMware Indexes	SA-VMWIndex-inframon or SA-VMWIndex		X			Creates indexes that store vCenter log data.

* If you send syslog data directly to the indexer.

† If you send syslog data directly to the Data Collection Node (DCN).

Install Splunk Add-on for vCenter Logs in a on-cloud environment

This deployment diagram and corresponding table outline the full installation of Splunk Add-on for vCenter Logs in a cloud environment.


vCenter
VMware
VMware Infra
vCenter Logs
Intermediate Forwarder
(syslog)
Event Data
Indexer
Splunk Add-on
(Splunk_TA_vce
Splunk Add-on
OR Splunk Add-

Add-on	Package	Search head	Indexer	Data collection node (DCN) or intermediate forwarder	Dedicated vCenter forwarder	The operation performed by the pacakage
Splunk Add-on for vCenter Logs	Splunk_TA_vcenter	X		X	X	Handles log data collection and parsing of vCenter logs.
Splunk Add-on for VMware Metrics Indexes or Splunk Add-on for VMware Indexes	SA-VMWIndex-inframon or SA-VMWIndex		X			Creates indexes that store vCenter log data.

As of vCenter 6.0, installation of a forwarder on your vCenter server for log forwarding is not recommended as a best practice for VMware. Instead, forward vCenter application logs to syslog, an intermediate forwarder, or directly to a Splunk indexer.

Set up your system for the Splunk Add-on for vCenter Logs

Configure ports to collect log data from the vCenter server

Review this information on how the entities in an 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 package on the vCenter Server system. If firewall issues prevent you from installing the Splunk Add-on for vCenter Logs 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.
vCenter server	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<add-link>

Set up add-on dependencies

The Splunk Add-on for vCenter logs receives the vCenter logs data via syslog/universal forwarder installed on the vCenter server and the data is ingested in the vmware-vclog index. The definition for the required index is present in the Splunk Add-on for VMware Metrics Indexes package or the Splunk Add-on for VMware Indexes package. If you are using Splunk Add-On for VMware Metrics you have to install the indexes package by following the Install and Configure Splunk Add-on for VMware Metrics Indexes steps. If you are using Splunk Add-On for VMware you have to install the indexes package by following the Install and Configure Splunk Add-on for VMware Indexes steps.

Install the Splunk Add-on for vCenter Logs

The Splunk Add-on for vCenter logs receives the vCenter logs data via syslog/universal forwarder installed on the vCenter server and the data is ingested in the vmware-vclog index. The definition for the required index is present in the Splunk Add-on for VMware Metrics Indexes package or the Splunk Add-on for VMware Indexes package. If you are using Splunk

Add-On for VMware Metrics you have to install the indexes package by following the Install and Configure Splunk Add-on for VMware Metrics Indexes steps. If you are using Splunk Add-On for VMware you have to install the indexes package by following the Install and Configure Splunk Add-on for VMware Indexes steps.

Install the Splunk Add-on for vCenter Logs to the environment tier to collect data.

Install Splunk Add-on for vCenter Logs to a cloud environment

1. Log in to your search head.
2. On the Splunk Web home page, select the gear icon next to **Apps**.
3. Select **Browse More Apps**.
4. Search for the "Splunk Add-on for vCenteri logs" and select **Install**.
5. Enter your Splunk.com login credentials.
6. Read and accept the terms and conditions, and select **Login and Download**.
7. Go to **Apps** > **Manage Apps** to review the installed app on the **Apps** page.

The vmware-vclog index, which is part of the SA-VMWIndex-inframon, package is required. If you are using Splunk Add-On for VMware Metrics you have to install the Splunk Add-on for VMware Metrics Indexes package. If you are using Splunk Add-On for VMware you have to Install the Add-on for VMware Indexes package.

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

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. You don't need to install anything on the vCSA servers to collect this data. Windows-based vCenter environments require a Splunk platform forwarder and the splunk_TA_vcenter package.

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 Metrics and 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 data connection node (DCN) polls vCenter server systems for performance, hierarchy, inventory, task, and event data. These credentials are required for DCN configuration. You can use an existing vCenter server account credentials, or create a new account for the Splunk App for VMware to access the vCenter server data.

If you encounter issues setting the correct permissions for vCenter server accounts, go to the User account permissions in the Splunk Add-on for VMware Metrics manual.

You have to 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, go to Create users in ActiveDirectory in this topic.

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

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

1. Log in to the Windows OS with an administrator account.
2. Select **Start** > **Control Panel**.
3. On the **User Accounts** screen, select **Add or remove user accounts**.
4. In the **Manage Accounts** window, select **Create a new account**.
5. Enter a name for the account, for example, splunksvc.
6. In vSphere, select **Standard user**.
7. Select **Create Account**.
8. On the **Manage Accounts** screen, select the new user.
9. On the **Change an Account** screen, select **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. Verify that you 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 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.

The steps to 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. Select **Home** in the path bar.
4. Under **Administration** select **Roles** > **Add Role**.
5. On the **Add new Role** screen, enter a name for the role, for example, splunkreader.
6. Select the appropriate permissions for the role.

Configure DCNs to honor TLS protocols

You might need to set your DCNs to honor TLS protocols when making requests to the vCenter APIs.

1. On your DCN, navigate to $SPLUNK_HOME\etc\system\local.
2. Open the web.conf file with a text editor. If there is no web.conf file, create the file.
3. Add this stanza 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. Go to the known issues in the release notes the Splunk Add-on for VMware Metrics for details on 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. Go to the VMware Knowledge Base for detailed installation instructions.

- 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 vCenter Logs 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. For instructions, go to Install a Universal Forwarder on Windows.
2. 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. Go to Configure forwarding with outputs.conf.
3. Change your Splunk password. The default password for the Splunk Enterprise admin user is changeme. Change the password using Splunk Web. Go to Change a password.
4. Install the Splunk_TA_vcenter package:
    1. Download Splunk Add-on for vCenter Logs from Splunkbase and extract its components.
    2. Copy the Splunk_TA_vcenter package from the extracted components 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's C:\Program Files\Splunk\etc\apps.
5. Install the Splunk_TA_vCenter package in the system where you have installed the Splunk Enterprise forwarder.
6. Copy the inputs.conf file from the $SPLUNK_HOME\etc\Splunk_TA_vCenter\default directory
7. Paste the inputs.conf file into the $SPLUNK_HOME\etc\Splunk_TA_vCenter\local directory.
8. Open the local inputs.conf file.
9. Change the log path to the location of the vCenter Server Appliance logs data, C:\ProgramData\VMware\vCenterServer\logs. Edit these 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
```

10. (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.
    1. Copy the $SPLUNK_HOME\etc\Splunk_TA_vCenter\default\props.conf file.
    2. Paste $SPLUNK_HOME\etc\Splunk_TA_vCenter\default\props.conf into the $SPLUNK_HOME\etc\Splunk_TA_vCenter\local directory.
    3. Open the local props.conf file.
    4. Change the log path to that in which the vCenter Server Appliance logs data. Edit these stanzas in the props.conf file:
       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 ¦]
```

11. Restart Splunk Enterprise. Go to Start and stop Splunk in the Admin Manual.
12. 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 vCenter Logs 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 vCenter Logs 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 where you have installed Splunk Enterprise.
- Install a Splunk Enterprise forwarder on the same machine to forward the VMware vCenter Linux appliance logs. For more information, go to the Forward VMware vCenter Linux appliance logs to Splunk Enterprise section of this page.

Export vCenter logs to an external system

1. Install a Splunk forwarder.
    1. Download the universal forwarder.
    2. Install the Splunk universal forwarder. Go to the Install the universal forwarder documentation for installation steps.
2. 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 light forwarder. Go to NFS Storage on the VMware vCenter Server Appliance in the VMware vSphere documentation.
3. Install the Splunk_TA_vCenter package on the system where you have installed the Splunk Enterprise forwarder.
4. Copy the inputs.conf file from $SPLUNK_HOME\etc\Splunk_TA_vCenter\default.
5. Paste the inputs.conf file into the $SPLUNK_HOME\etc\Splunk_TA_vCenter\local directory.
6. Open the local inputs.conf file.
7. Edit these stanzas in the inputs.conf file to change the log path to the location that stores the vCenter Server Appliance logs data (/var/log/vmware/).

Linux server appliance 6.x and 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 5.x (not supported from 3.4.5)

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

8. (Optional) If you configured Splunk Enterprise as a heavy or light forwarder and you want to monitor the license file and tomcat configuration files.
    1. Copy the $SPLUNK_HOME\etc\Splunk_TA_vCenter\default/props.conf file.
    2. Paste in the $SPLUNK_HOME\etc\Splunk_TA_vCenter\local directory.
    3. Open the local props.conf file.
    4. Edit these stanzas to change the log path to where the vCenter Server Appliance logs data is stored:

    Linux server appliance 6.x and 7.0

    ```
    [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+)?]
    ```

9. 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 has to be enabled.

1. Install a Splunk forwarder on the VMware vCenter Server Appliance.
2. Install the Splunk_TA_vCenter package on the Splunk platform forwarder.
    1. Download Splunk Add-on for vCenter Logs from Splunkbase and extract its components.
    2. Copy the Splunk_TA_vcenter package from the extracted components to $SPLUNK_HOME\etc\apps directory.
3. Copy the inputs.conf file from $SPLUNK_HOME\etc\Splunk_TA_vCenter\default.
4. Paste the inputs.conf file in the $SPLUNK_HOME\etc\Splunk_TA_vCenter\local directory.

5. Open the local inputs.conf file.
6. (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 directory.
7. 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

vCenter 5.5 is not supported from VMware 3.4.5.

Syslog-ng on vCenter 5.5

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

1. Open your vCenter deployment, and navigate to \etc\syslog-ng\.
2. Open the \etc\syslog-ng\syslog-ng.conf file.
3. 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, run the command `service syslog restart` to restart the syslog service for the changes to take effect.

5. Navigate to Splunk\etc\apps\Splunk_TA_vcenter\ and create a local directory.
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 this stanza:

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

8. Open the Splunk\etc\apps\Splunk_TA_vcenter\local\inputs.conf file.
9. Paste the copied stanza in the local inputs.conf file.
10. Uncomment the copied stanza to enable it.

> Note: Since TCP port 1514 is used for receiving ESXi logs, the 1517 port is used by default for vclogs. You can use another open port.

File properties	Description
flags	Used to forward the log without any parsing.
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.

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

Rsyslog on vCenter 6.x

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

1. Open your vCenter deployment, and navigate to the \etc\ directory.
2. Open the rsyslog.conf file.
3. 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, run the command `service syslog restart` to restart the syslog service for the changes to take effect.
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.
9. Paste the copied stanza into the local version of inputs.conf.
10. Enable the copied stanza in local/inputs.conf by uncommenting it.

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.
$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, go to the text file input module page in the Rsyslog documentation.

Reference

Troubleshoot the Splunk Add-on for vCenter Logs

The Splunk Add-on for vCenter Logs isn't receiving data

Problem

The Splunk Add-on for vCenter Logs isn't receiving data.

Cause

If you've 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.

Solution

Resolve this issue by installing the missing VMware WSDL files as documented in the vSphere Web Services SDK WSDL workaround in the VMware documentation.

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

Note that the program data folder is typically a hidden folder.

Source types for the Splunk Add-on for vCenter Logs

The Splunk Add-on for vCenter Logs collects data from the following sources via syslog.

Type of data	Source	Source type	Collection method
vCenter logs	.../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

Third-Party Software

Credits

There is no third-party library used in Splunk Add-on for vCenter Logs.