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

Generated: 11/05/2022 12:00 pm

Table of Contents

Overview

About the Splunk Add-on for VMware ESXi Logs

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

The Splunk Add-on for VMware ESXi Logs contains the input stanzas to receive the data from the syslog and search-time/index-time extractions and parses and extracts the fields from the VMware ESXi logs. It accepts ESXi log data using syslog which allows you to troubleshoot events and host issues.

The package included in Splunk Add-on for VMware ESXi Logs (Splunk_TA_esxilogs) was previously part of Splunk Add-on for VMware Metrics in v4.2.0 or previous and the Splunk Add-on for VMware in v4.0.2 or previous. This package is published as the Splunk Add-on for ESXi 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 and the Splunk Add-on for VMware 4.0.3.

Download the Splunk Add-on for VMware ESXi Logs from Splunkbase at https://splunkbase.splunk.com/app/5603/.

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

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

The package included in Splunk Add-on for VMware ESXi logs (Splunk_TA_esxilogs) was previously part of Splunk Add-on for VMware Metrics in v4.2.0 or previous and the 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 and the Splunk Add-on for VMware v4.0.3 in cloud environments.

What's new

These features are available in the Splunk Add-on for VMware ESXi 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 ESXi log data	The package contains the search-time and index-time extractions to parse and extract fields from the VMware ESXi logs forwarded using syslog.
Support for self-service installation in cloud environments	Customers of the Splunk Add-on for VMware Metrics or Splunk Add-on for VMware in a 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 below and Splunk Add-on for VMware v4.0.2 or below, existing customers of Splunk Add-on for VMware Metrics have to follow the upgrade steps for the Splunk Add-on for VMware Metrics to

New feature or enhancement	Description
	switch to the version of the add-on that supports self-service installation. Existing customers of 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 the self-service installation.

Fixed issues

This version of the Splunk Add-on for VMware ESXi 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 ESXi 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 VMware ESXi Logs

Latest release

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

Installation and Configuration

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

Before you deploy the Splunk Add-on for VMware ESXi 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 ESXi logs data from the forwarder is stored in this index. The Splunk Add-on for ESXi Logs package indexes the data into the vmware-esxihost index. 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-esxihost	Stores ESXi host log data.

Data volume requirements

The expected ESXi logs data volume ingested by this package in a typical environment is 125-235 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
ESXi host logs	135-235 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 VMware ESXi Logs version	Compatible Splunk Add-on for VMware Metrics Indexes version	Compatible vCenter version	Compatible ESXi version

Splunk Add-on for VMware Metrics version	Compatible Splunk Add-on for VMware ESXi 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 VMware ESXi 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 VMware ESXi Logs

The Splunk Add-on for ESXi Logs can't forward esxilogs to indexers in a cluster. The workaround for this is in Troubleshoot the Splunk Add-on for VMware ESXi Logs.

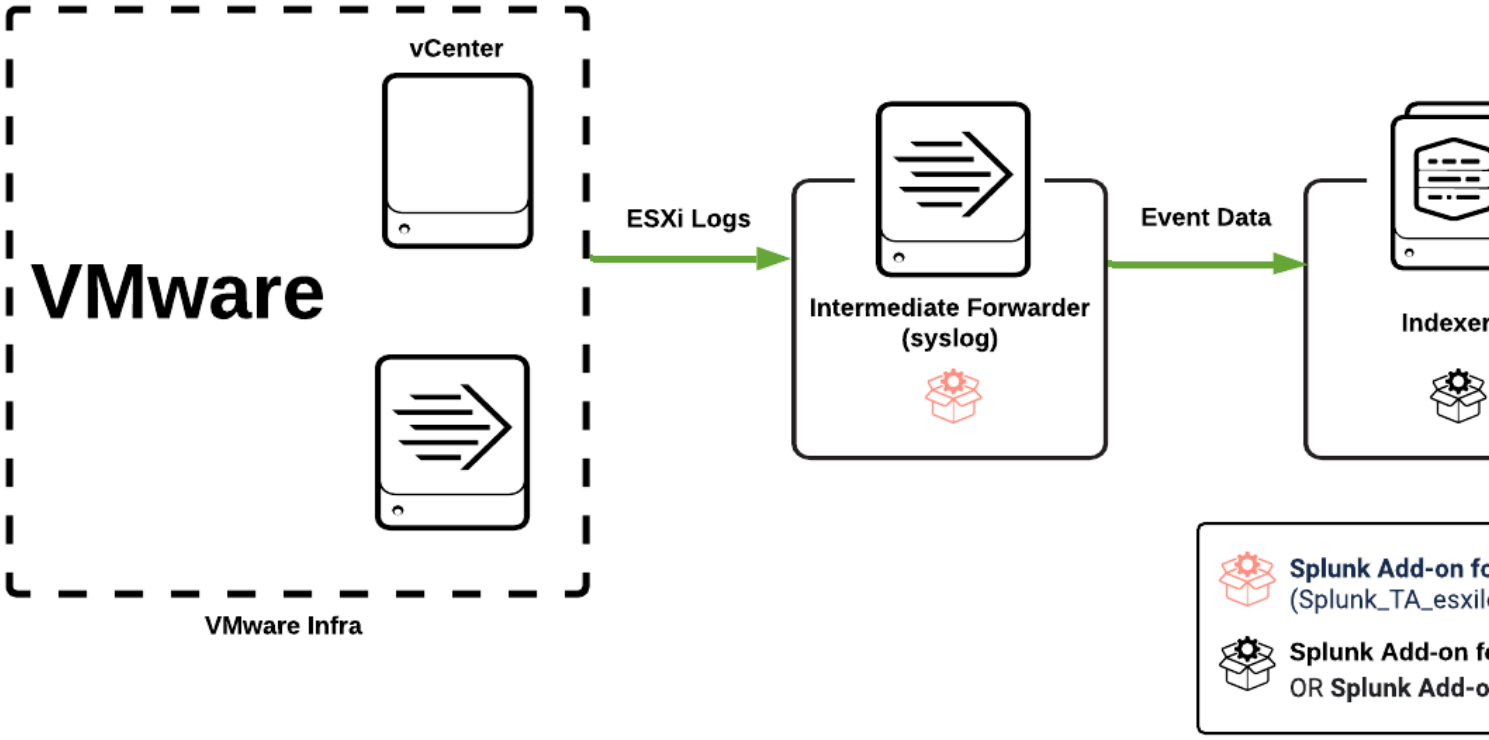
The Splunk Add-on for VMware ESXi logs package contains the necessary index-time and search-time extractions to parse the ESXi logs collected using the syslog. This overview outlines a full installation of the Splunk Add-on for VMware ESXi Logs on a distributed deployment.

Install the Splunk Add-on for VMware ESXi Logs

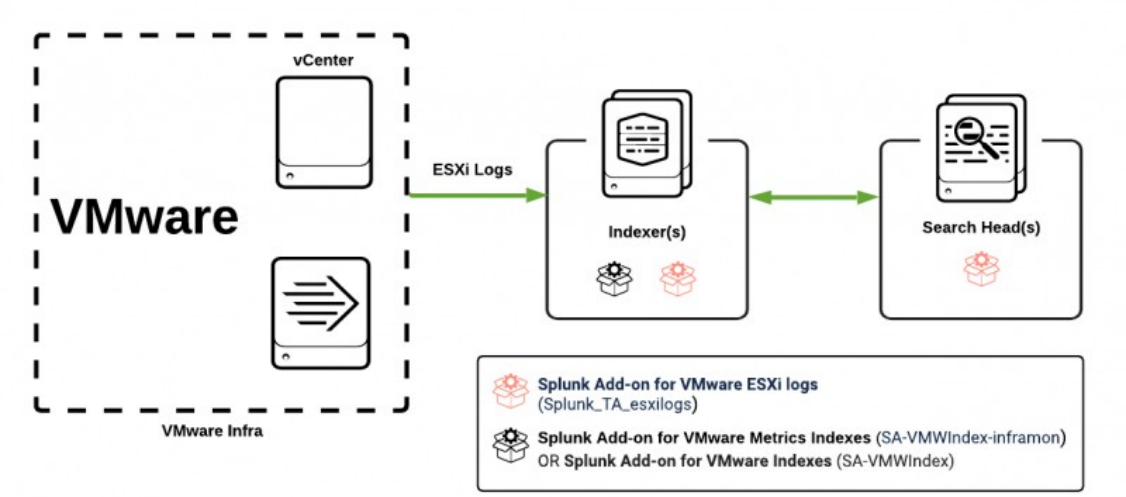
Review the deployment diagram and corresponding table for your environment type for details on the install locations for each VMware ESXi logs data collection package. If you are using an on-premises environment, you can forward the data directly to the indexer or using an intermediate forwarder (such 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 VMware ESXi Logs in an on-premises environment

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


vCenter
VMware
VMware Infra
ESXi Logs
Intermediate Forwarder
(syslog)
Event Data
Indexer
Splunk Add-on fo
(Splunk_TA_esxil
Splunk Add-on fo
OR Splunk Add-o

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



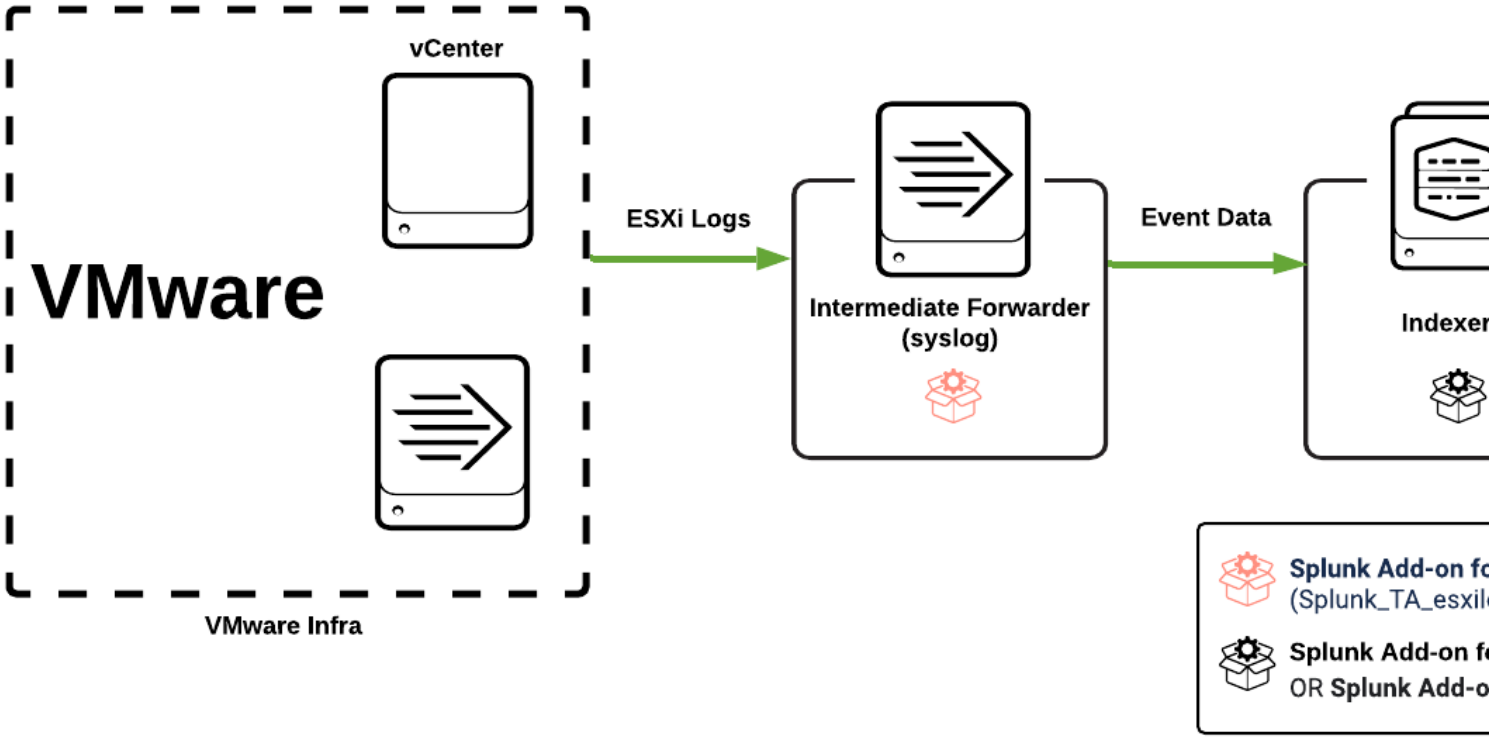
Add-on	Package	Search head	Indexer	Data collection node (DCN)	Dedicated ESXi forwarder	The operation performed by the pacakage
Splunk Add-on for ESXi Logs	Splunk_TA_esxilogs	X	X*	X†	X	Handles log data collection and parsing from ESXihosts.
Splunk Add-on for VMware Metrics Indexes or Splunk Add-on for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

* 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 VMware ESXi Logs in a Cloud environment

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


vCenter
VMware
VMware Infra
ESXi Logs
Intermediate Forwarder
(syslog)
Event Data
Indexer
Splunk Add-on fo
(Splunk_TA_esxil
Splunk Add-on fo
OR Splunk Add-o

Add-on	Package	Search head	Indexer	Data collection node (DCN) or intermediate forwarder	Dedicated ESXi forwarder	The operation performed by the pacakage
Splunk Add-on for ESXi Logs	Splunk_TA_esxilogs	X		X	X	Handles log data collection and parsing from ESXihosts.
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 ESXi log data forwarded by VMware ESXi hosts.

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

Configure ports to collect log data from the ESXi hosts

Review this information on how the entities in an environment communicate.

Sender	Receiver	Port number	Description
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 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 with the Splunk_TA_esxilogs add-on package installed. Alternatively, you can send syslog to another DCN virtual machine dedicated to run as a Syslog server for the ESXi hosts.

Set up add-on dependencies

Splunk Add-on for VMware ESXi Logs receives the ESXi logs data via syslog and the data is ingested in the vmware-esxilog 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 depending on the VMware add-on you are using. If you are using the Splunk Add-on for VMware Metrics, you have to install the metrics indexes package by following the steps in Install and Configure Splunk Add-on for VMware Metrics Indexes. If you are using Splunk add-on for VMware, follow the steps in Install and Configure Splunk Add-on for VMware Indexes.

Install and configure the Splunk Add-on for VMware ESXi Logs

ESXi server logs allow you to troubleshoot events and host issues. Splunk Add-on for VMware ESXi logs accepts ESXi log data using syslogs from these 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 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 universal forwarder.
2. Install the Splunk universal forwarder. Go to the Install the universal forwarder documentation for installation steps.

Step 2: Create an inputs.conf file

1. Create an inputs.conf file.
2. Save the file to the system/local directory to monitor the ESXi hosts log files on the syslog server.
3. For each monitor stanza in the inputs.conf file, specify these settings:
   - `index = vmware-esxilog`
   - `sourcetype = vmw-syslog`

   The entry in the monitor stanza of the inputs.conf file looks like this:

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

4. 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 the Splunk_TA_esxilogs package is installed. For more information about setting up forwarding for your indexers, go to Configure forwarders with outputs.conf.

Step 3: Install the Splunk_TA_esxilogs package

Download Splunk Add-on for VMware ESXi Logs from Splunkbase and the build will have Splunk_TA_esxilogs package in it. Install the Splunk_TA_esxilogs package on the machine that receives log data from your syslog server in the $SPLUNK_HOME/etc/apps directory.

Step 4: Configure the Splunk_TA_esxilogs package

1. Assign the host field on the machine where you installed the Splunk_TA_esxilogs package. The Splunk Add-on for VMware ESXi logs can't 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 hostname 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 isn't required when you use an intermediate forwarder, as the Splunk App for VMware automatically assigns the host based on the original data source.
3. Create a local version of props.conf and transforms.conf files.
4. Save the files to 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 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. Don't override these fields in the local versions of these files.

This is an example of the entry for props.conf:

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

This is an example entry for transforms.conf:

```
[set_host]
REGEX = ^(?:\w{3}\s+\d+\s+[\d\:]{8}\s+([^ ]+)\s+)
DEST_KEY = MetaData:Host
FORMAT = host::$1
```

5. If the sourcetype isn't correct, check the regular expressions in the `[set_syslog_sourcetype]` and `[set_syslog_sourcetype_4x]` stanzas in Splunk_TA_esxilogs/default/transforms.conf.

   This is an example of an entry in transforms.conf 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 the host field and `([A-Za-z\-]+)` is used to extract the sourcetype.

```
[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
```

Troubleshoot the Splunk_TA_esxilogs package

- If the time isn't 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 don't display in the ESXi Log Browser, modify the regular expressions in the [esx_vmkernel_fields] and [esx_generic_fields] stanzas.
  This is an example of the 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 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 package and extract its contents to SPLUNK_HOME/etc/apps/ directory.

Step 2: Enable the ports to receive syslog data

Enable ports in Splunk Web or by modifying the inputs.conf file.

Use UDP port 514. As the Splunk user on the intermediate forwarder, you have to have root privileges to configure data inputs. If you do not have the required privileges, use TCP port 1514.

Enable ports in Splunk Web

1. Select **Settings** > **Data Inputs**.
2. Select **TCP** > **New Local TCP**.
3. Enter 1514 in **Port**.
4. Select **Next**.
5. On the **Input Settings** enter this info:
    - **Source type**: New
    - **Source Type**: vmw-syslog
    - **App Context**: Splunk Add-on for ESXi logs
    - **Method**: DNS
    - **Index**: vmware-esxihost
6. Select **Review** and **Submit**.

*This is the destination for the syslog data. Set the destination index for the source after you have installed the Splunk App for VMware components.

Enable ports in the inputs.conf file

If you don't have access to Splunk Web you can enable ports in the inputs.conf file.

1. Create an inputs.conf file in the $SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/local/ directory.
2. Copy this 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
```
3. Paste the stanza in your new inputs.conf file in the $SPLUNK_HOME/etc/apps/Splunk_TA_esxilogs/local/ directory.
4. Uncomment the stanza in the inputs.conf of local directory.

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. Go to the **Configuration** tab.
3. In the **Software** section, select **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 a comma between the two machine specifications. For example, enter tcp://yourmachine1.yourdomain:1514, tcp://yourmachine2.yourdomain:1514.
    - vSphere version 4.1 only forwards to TCP. In this case, don't 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. Select **OK**.
7. In **Software**, select **Security Profile**.
8. In **Firewall**, select **Properties**.
9. In **Firewall Properties Remote Access**, select **Syslog**.
10. Select **Firewall**.
11. Select **Allow connections from any IP address** or specify the connections.
12. Select **OK**.

Set up a host profile

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

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

Install Splunk Add-on for VMware ESXi logs to a cloud environment

The Splunk add-on for VMware ESXi Logs is required on the search head tier in cloud environments for search-time extraction. Follow these steps

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 VMware ESXi 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-esxihost index, which is part of the SA-VMWIndex-inframon or SA-VMWIndex, the package is required. If you are using Splunk Add-on for VMware Metrics, download the Splunk Add-on for VMware Metrics Indexes to obtain the SA-VMWIndex-inframon, package. If you are using the Splunk add-on for VMware, download the Splunk Add-on for VMware Indexes to obtain the SA-VMWIndex package.

Reference

Troubleshoot the Splunk Add-on for VMware ESXi Logs

Not getting esxilogs

Problem

Not getting esxilogs while forwarding it to indexers which are in a cluster in the on-premise deployment. You might also see this error message splunkd.log on indexers:

```
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 the cluster), splunkd.log on indexers will show this error:

Splunk is not able to find a custom timestamp parser file (syslog_datetime.xml) which is used to extract dates and timestamps from events.

The following parameter is set for this in props.conf file present in the Splunk_TA_esxilogs package:

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

As indexers are in the cluster, Splunk_TA_esxilogs on indexers would be installed under slave-apps (/etc/slave-apps/) hence the path wouldn't exist. Note that as per the deployment guideline for the Splunk Add-on for VMware ESXi logs, if you are forwarding the ESXi logs in the cloud environment, you have to install the "Splunk_TA_esxilogs" package on the intermediate forwarder, and thus it wouldn't be needed on the indexer. Therefore, this issue can't occur in the cloud environment.

Solution

1. On cluster master, create a local directory in the $SPLUNK_HOME/etc/master-apps/Splunk_TA_esxilogs directory, if not present.
2. Create a props.conf file in the $SPLUNK_HOME/etc/master-apps/Splunk_TA_esxilogs/local directory (if not present) and add this setting:

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

Source types for the Splunk Add-on for VMware ESXi logs

The Splunk Add-on for VMware ESXi logs collects data from the following sources via Syslog.

Type of data	Source	Source type	Collection method
ESXi logs	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
		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:ImageConfigManager	File monitoring
		vmware:esxlog:Rhttpproxy	File monitoring
		vmware:esxlog:storageRM	File monitoring
		vmware:esxlog:root	File monitoring
		vmware:esxlog:sfcb-hhrc	File monitoring

Third-Party Software

Credits

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