Table of Contents

Introduction..................................................................................................................1
   About the Splunk App for VMware........................................................................1

Set up your system for Splunk App for VMware..................................................2
   Platform and hardware requirements...................................................................2
   Plan your installation in a test environment.......................................................6
   Set up a vCenter Server user account...............................................................7
   Validate vCenter Servers time synchronization settings.....................................7
   Configure ports.....................................................................................................8
   Prepare to host a data collection node...............................................................10
   Prepare Splunk App for NetApp Data ONTAP....................................................11

Install and deploy Splunk App for VMware.........................................................12
   Installation overview..........................................................................................12
   Install the Splunk App for VMware.................................................................14
   Configure license...............................................................................................18
   Assign user roles for Splunk App for VMware..................................................21
   Deploy the Splunk OVA for VMware to create a Data Collection Node..............21
   Configure the data collection node and system settings.....................................22
   Configure Splunk App for VMware to collect data from vCenter Server............22
   Collect VMware vCenter Server Linux Appliance log data...............................24

Troubleshoot...........................................................................................................26
   Troubleshoot Splunk App for VMware..............................................................26
   Upgrade from tsidx namespaces to data model acceleration.............................33
   Set Splunk App for VMware trial license to work with remote license master..........................................................40

Upgrade Splunk App for VMware..........................................................................42
   Upgrade to Splunk App for VMware 3.4.4.........................................................42
Introduction

About the Splunk App for VMware

The Splunk App for VMware provides real-time visibility into the health of virtual environments. It leverages the Splunk platform to collect metrics, logs, tasks, events, and topology from hosts, virtual machines, and virtual centers. It identifies performance and capacity bottlenecks from the following sources:

- Storage for data stores, such as SAN or NAS
- Network devices providing the networking backbone of the virtualization environment
- Authentication logs from sources such as Active Directory, LDAP, and so on
- DNS, DHCP, BootP logs
- Operating system and application logs from virtual machines

Supported VMware operating environments

Use the table to identify which operating environment works with each Splunk platform component within the Splunk app for VMware.

<table>
<thead>
<tr>
<th>Component</th>
<th>Linux Supported</th>
<th>Windows Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Head</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Indexer</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DCN</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Forwarder (Universal, Heavy, Light)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Download the Splunk App for VMware

1. Download the Splunk App for VMware package from Splunkbase and accept the license agreement.
2. Confirm the contents of the download package,
   splunk_app_for_vmware-<version>-<buildnumber>.tgz.

   - splunk_app_vmware-<version>-<build_number>
   - SA-Threshold
   - SA-VMW-HierarchyInventory
   - SA-VMW-LogEventTask
   - SA-VMW-Performance
Set up your system for Splunk App for VMware

Platform and hardware requirements

Splunk App for VMware works on Splunk platform instances deployed in a *nix environment. Windows is not a supported operating system for this app.

The Splunk App for VMware supports vCenter Server systems in Linked Mode. Splunk App for VMware collects API data for vCenter Server systems in a linked pool after you add them to the Collection Configuration dashboard in the Splunk Add-on for VMware. The Splunk Add-on for VMware does not recognize vCenter Servers in a linked pool that are not included in the data collection configuration.

The image shows how VMware is installed across a Splunk platform deployment.
• See System requirements in the Splunk Enterprise Installation Manual.
• Plan your deployment according to the capacity planning guidelines in Splunk Enterprise capacity planning.
• If your deployment includes NetApp devices, install and configure Splunk App for NetApp Data ONTAP before you install Splunk App for VMware. See Prepare your Splunk App for NetApp.

Supported browsers
• Mozilla Firefox
• Microsoft Internet Explorer 9 and above
• Apple Safari
• Google Chrome

The Splunk App for VMware does not support Internet Explorer 8 or Internet Explorer 9 Compatibility Mode.

Splunk App for VMware Installation Prerequisites

Installation of the Splunk App for VMware has the following prerequisites.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk platform</td>
<td>A configured and ready to use Splunk platform environment.</td>
</tr>
<tr>
<td>A search head that runs on a 64-bit Linux system.</td>
<td>Your Splunk environment can be a single-instance deployment, or a deployment with a dedicated search head and one or more indexers.</td>
</tr>
<tr>
<td>A Splunk platform license</td>
<td>A default Splunk platform configuration with a licensing volume that can support approximately 300MB of data per host per day.</td>
</tr>
<tr>
<td>Use of a supported version of VMware vCenter Server to manage hypervisors.</td>
<td>Splunk App for VMware integrates with a vCenter Server and the hypervisors it manages. Environments with Windows-based vCenter and/or Linux-based vCenter Server Appliance are supported. ESXi servers that are not managed through vCenter are not supported.</td>
</tr>
<tr>
<td>Installation and configuration of the Splunk Add-on for VMware</td>
<td>Installation of the Splunk Add-on for VMware is necessary to collect and transform data from VMWare vCenters, ESXi hosts and Virtual Machines. See Installation and Configuration of the Splunk Add-on for</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Installation and configuration of the Splunk OVA for VMware</td>
<td>The Splunk OVA for VMware collects and harnesses Data Collection Node (DCN) data from the virtualization layer to enable functionality with Splunk IT Service Intelligence, the Splunk Add-on for VMware and the Splunk App for VMware. See Installation and Configuration of the Splunk OVA for VMware for DCN installation and configuration information.</td>
</tr>
</tbody>
</table>

### Component version compatibility

See the table to identify component version compatibility for your Splunk VMware deployment.

<table>
<thead>
<tr>
<th>Compatible Splunk platform version</th>
<th>Compatible Splunk App for VMware version</th>
<th>Compatible vCenter version</th>
<th>Compatible vSphere version</th>
<th>Compatible ESXi version</th>
<th>Compatible SA-Hydra version</th>
<th>Compatible SA-VMWNetAppUtils version</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.0 through 6.4.3</td>
<td>3.2.1 to 3.3.0</td>
<td>5.0 to 6.0</td>
<td>4.1, 5.0, 5.0</td>
<td>4.1, 5.0, 5.0</td>
<td>4.0.2 and above</td>
<td>3.5.0, 3.7.0</td>
</tr>
<tr>
<td>6.3 to 6.5</td>
<td>3.3.1</td>
<td>5.0 to 6.0</td>
<td>4.1, 5.0, 5.0</td>
<td>4.1, 5.0, 5.0</td>
<td>4.0.2 and above</td>
<td>3.5.0, 3.7.0</td>
</tr>
<tr>
<td>6.3 to 6.5</td>
<td>3.3.2</td>
<td>5.0, 6.0, 6.5</td>
<td>4.1, 5.0, 5.0</td>
<td>4.1, 5.0, 5.0</td>
<td>4.0.4</td>
<td>1.0.0 (Vers 3.3.2 replaces SA-Utils with SA-VMNetAppUtils)</td>
</tr>
<tr>
<td>6.4 to 6.6</td>
<td>3.4.0</td>
<td>5.5, 6.0, 6.5</td>
<td>5.5, 6.0, 6.5</td>
<td>5.5, 6.0, 6.5</td>
<td>4.0.5</td>
<td>1.0.1</td>
</tr>
<tr>
<td>6.5 to 7.0</td>
<td>3.4.1</td>
<td>5.5, 6.0, 6.5</td>
<td>5.5, 6.0, 6.5</td>
<td>5.5, 6.0, 6.5</td>
<td>1.0.2 and above</td>
<td>1.0.3</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Collected data type</th>
<th>Data volume</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total vCenter logs</strong></td>
<td>15 MB of data per host per day per vCenter. For example, 750MB in a 50 host environment.</td>
</tr>
<tr>
<td><strong>ESXi host logs</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Total API data per host</strong></td>
<td>10 MB of data per host per day.</td>
</tr>
<tr>
<td><strong>Total API data per virtual machine</strong></td>
<td>3 MB of data per day.</td>
</tr>
</tbody>
</table>

### Scheduler requirements

The Splunk App for VMware uses the Splunk Add-on for VMware to install and manage distributed collection scheduling (previously contained in the Splunk App for VMware component bundle), and to deploy the python script `splunk_for_vmware_setup.py` that collects DCN details, such as DCN URI, username, and password information from the Collection Configuration page, before sending them to SA-Hydra.
For single deployments of the VMware app scheduler, see the SplunkEnterprise
search head hardware recommendations.

If you have Splunk App for NetApp ONTAP installed, it also uses the Collection
Configuration page. See Prepare Splunk App for NetApp Data ONTAP of the

Plan your installation in a test environment

Install the Splunk App for VMware into a test environment before you install it in a
production environment. You can work out the complexities and issues that you
might encounter in your deployment.

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

If you do not 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 App 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 Splunk App for VMware.
- One Data Collection Node (DCN).

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
App 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 App for VMware. This action is not required for a working VMware app deployment. See Configure the Splunk Add-on for VMware to collect log data from ESXi hosts.

See "Deploy OVA to create a Data Collection Node" section of Splunk OVA for VMware. For information about configuring Splunk App for VMware with other Splunk apps, see Requirements for installing the Splunk App for VMware with other Splunk apps.

**Set up a vCenter Server user account**

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

These credentials allow the Splunk App 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 have problems setting the correct permissions for vCenter Server accounts, see "Permissions in vSphere."

**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 App for VMware relies on the Splunk Add-on for VMware to use the VMware API to collect data about your virtual environment. The Splunk Add-on for VMware communicates 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.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Configuration</td>
<td>vCenter server</td>
<td>443</td>
<td>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.</td>
</tr>
<tr>
<td>Splunk Add-on for VMware</td>
<td>Data Collection Node</td>
<td>8089</td>
<td>Connects to the Data Collection Node (DCN) on the default Splunk management port, TCP 8089.</td>
</tr>
<tr>
<td>Collection Configuration</td>
<td>Data Collection Node</td>
<td>8008</td>
<td>When the DCN and Splunk App 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).</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection Node (DCN)</td>
<td>vCenter Server</td>
<td>443</td>
<td>Communicates with vCenter Server API on port 443 to execute the data collection tasks allocated to it.</td>
</tr>
<tr>
<td>Data Collection Node</td>
<td>Splunk indexer</td>
<td>9997</td>
<td>Uses port 9997 to forward data it has retrieved from the vCenter Server using the API.</td>
</tr>
</tbody>
</table>

After Splunk App 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. 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.

**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.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter server</td>
<td>Splunk indexer</td>
<td>9997</td>
<td>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</td>
</tr>
</tbody>
</table>
installing the Splunk App for VMware 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.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi host</td>
<td>DCN/Syslog server</td>
<td>TCP port 1514 / UDP port 514</td>
<td>Prior to ESXi version 5.5, 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 DCN. 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.</td>
</tr>
</tbody>
</table>

**Prepare to host a data collection node**

The Splunk App 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.

Splunk configures the DCN with the following default configuration:

- Four cores. 4 vCPUs or 2 vCPUs with two cores with a reservation of 2GHz.
- 6GB memory with a reservation of 1GB.
- 10-12GB 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 40 or fewer ESXi hosts, based on the specifications for the 4 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 will eventually fail at some point. 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.

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

Prepare Splunk App for NetApp Data ONTAP

Splunk App for NetApp Data ONTAP and Splunk App for VMware share the Collection Configuration dashboard to manage data collection tasks, SA-Hydra and SA-Utils.

If you do not have the Splunk App for NetApp Data ONTAP installed in your environment, skip this step and proceed to download and install the Splunk App for VMware.

Splunk App for NetApp 2.0.x or earlier

If you have Splunk App for NetApp Data ONTAP version 2.0.x or earlier installed in your test environment, upgrade the Splunk App for NetApp Data ONTAP’s Data Collection Node with SA-Hydra 4.0.2 and SA-Utils 3.7.0, which are bundled with the Splunk Add-on for VMware.
Install and deploy Splunk App for VMware

Installation overview

Installation of the Splunk OVA for VMware and Splunk Add-on for VMware are prerequisites for the Splunk App for VMware. The Splunk App for VMware cannot be installed using a GUI.

Splunk App for VMware package contents

The Splunk App for VMware contains the following components:

- SA-Threshold
- SA-VMware HierarchyInventory
- SA-VMware LogEventTask
- SA-VMW Performance
- Splunk for VMware

Install components

The table shows where to install the individual components of Splunk App for VMware in your distributed environment.

<table>
<thead>
<tr>
<th>Component</th>
<th>Search head</th>
<th>Scheduler</th>
<th>Indexer</th>
<th>Data Collection Node (DCN)</th>
<th>ESXi log forwarder</th>
<th>vCenter log forwarder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk_for_vmware</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk_TA_vmware</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk_TA_esxilogs</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk_TA_vcenter</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-VMW-HierarchyInventory</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-VMW-LogEventTask</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-VMW-Performance</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-Hydra</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-VMNetAppUtils</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-Threshold</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Forwarding vCenter application logs to syslog, an intermediate forwarder, or directly to a Splunk indexer is supported for 6.0 and 5.X versions of vCenter server. As of vCenter 6.0, installing a forwarder on your vCenter server for log forwarding is not necessary or recommended.

The installation of SA-VMNetAppUtils on your license server is optional if your Splunk platform deployment does not use a license server. If your search head handles licensing then SA-VMNetAppUtils should already be installed on your search head.

**Component reference**

Refer to this table to see the Splunk App for VMware components that are installed and where the components get installed in the Splunk Enterprise and VMware infrastructure.

<table>
<thead>
<tr>
<th>Component name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search head</td>
<td>If you have a dedicated search head, install all of the components except Splunk_TA_vmware and SA-VMWIndex on it. Install SA-Hydra and SA-VMNetAppUtils on distributed deployments. Installation of all components on the search head lets you view a complete working version of the app.</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Manages jobs. If you use SHC in your Splunk platform environment, run the scheduler on a separate machine from your SHC members.</td>
</tr>
<tr>
<td>Indexer</td>
<td>Install SA-VMWIndex dedicated indexer.</td>
</tr>
<tr>
<td>Data Collection</td>
<td>The data collection node OVA ships with all components installed. To build your own data collection node, see create your</td>
</tr>
</tbody>
</table>
Install the Splunk App for VMware

Versions 3.3.0 and above of the Splunk App for VMware use the Splunk OVA for VMware to create and deploy the data collection nodes (DCN), and the Splunk Add-on for VMware to manage the scheduler functionality that the Splunk App for VMware uses to collect and analyze virtual machine data. See the image to see how the Splunk App for VMware works with the Splunk OVA for VMware and the Splunk Add-on for VMware.

Follow the instructions below to install the Splunk App for VMware on your Splunk platform environment. For distributed environments, see the Install the Splunk App for VMware in a search head cluster environment section of the Install the Splunk App for VMware section of the Splunk App for VMware manual as reference for distributed deployments.

Install Splunk App for VMware on a full Splunk platform instance using the same user account credentials that you used to install your Splunk platform. For instructions on how to install Splunk App for VMware in a clustered indexer environment, see the Splunk platform configuration guide.

1. Get the splunk_app_for_vmware-<version>-<build_number>.tgz and splunk_add_on_for_vmware-<version>-<build_number>.tgz files, put them in $SPLUNK_HOME/etc/apps on your Splunk platform host.
2. Extract the Splunk App for VMware package.
   
   ```bash
   cd /opt/splunk/etc/apps
   tar xvzf splunk_app_for_vmware-*tgz
   ```

<table>
<thead>
<tr>
<th>Component name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>own data collection node <em>Splunk OVA for VMware</em>.</td>
</tr>
<tr>
<td>Esxi host</td>
<td>Install the log forwarding technology on the ESXi host. If you use an intermediate heavy forwarder to forward logs, install Splunk_TA_esxilogs on the forwarder.</td>
</tr>
<tr>
<td>vCenter server</td>
<td>Only install the log forwarding technology on the vCenter server. If you use a universal forwarder or light forwarder to forward vCenter logs, install Splunk_TA_vcenter on it as it contains scripts that configure the inputs.conf.</td>
</tr>
<tr>
<td>License Master</td>
<td>See &quot;Configure a license master&quot; in the Splunk Enterprise admin manual.</td>
</tr>
</tbody>
</table>
3. Verify that you extracted all of the sub directories in the $SPLUNK_HOME/etc/apps directory.

   From `tar xvzf splunk_app_for_vmware-*.tgz`:
   - SA-Threshold/
   - SA-VMW-HierarchyInventory/
   - SA-VMW-LogEventTask/
   - SA-VMW-Performance/
   - splunk_for_vmware/

   From `tar xvzf splunk_add_on_for_vmware-*.tgz`:
   - SA-VMNetAppUtils/
   - SA-Hydra/
   - Splunk_TA_vcenter/
   - Splunk_TA_vmware/
   - Splunk_TA_esxilogs/
   - SA-VMWIndex/
   - TA-VMW-FieldExtractions/

4. (Optional) Remove the SA-VMW-Licensecheck folder from the $SPLUNK_HOME\etc\apps folder if it exists.

5. Restart Splunk Enterprise.

   /opt/splunk/bin/splunk restart

**Install the Splunk App for VMware in a search head cluster environment**

Versions 3.2.0 and above of the Splunk App for VMware support search head cluster (SHC) environments. See the image for guidance on how the Splunk App for VMware is deployed across an SHC environment.
Prerequisites

- For Search Head Clustering, you need a minimum of three instances of Splunk Enterprise to serve as search head cluster members, and one additional instance that serves as a deployer, which you use to distribute apps and updated configurations to the cluster members.
- The data collection node (DCN) scheduler must be deployed on a dedicated search head, and not on any individual search head in the SHC.
- Each search head cluster member should be fresh install of Splunk and not re-purposed splunk instance.
- You migrated your settings from a Search Head Pool to a Search Head cluster. See Migrate from a search head pool to a search head cluster in the "Splunk Enterprise Distributed Search Manual".
- You have a licensed version of Splunk Enterprise installed and running in your environment.
- You have access to the Splunk App for VMware and permission to install it.
- You have configured your deployment's Data Model properties, located in datamodels.conf on your indexers. See Upgrade from tsidx namespaces to data model acceleration to learn more.
You must use the search head cluster **deployer** to distribute your configurations across your set of search head cluster members. **Install the Splunk App for VMware in a search head cluster environment**

1. Take the files `splunk_app_for_vmware` and `splunk_add_on_for_vmware` that you downloaded from Splunkbase and put in a temporary directory. This avoids overriding critical files.

   ```bash
   cp splunk_app_for_vmware-<version>-<build_number>.tgz /tmp
   cp splunk_add_on_for_vmware-<version>-<build_number>.tgz /tmp
   ```

2. Change to the `/tmp` directory, and extract the app and add-on packages.

   ```bash
   cd /tmp
   tar xvzf splunk_app_for_vmware-<version>-<build_number>.tgz
   tar xvzf splunk_add_on_for_vmware-<version>-<build_number>.tgz
   ```

3. Copy the unzipped files and move into your deployer's **apps** folder inside the **shcluster** folder.

   ```bash
   cp -r * $SPLUNK_HOME/etc/shcluster/apps/
   ```

4. Verify that all of the apps and the subdirectories were copied correctly and reside in the `$SPLUNK_HOME/etc/shcluster/apps` folder.

5. On your **deployer**, remove the `Splunk_TA_vmware` and `SA-VMWIndex` folders from the `$SPLUNK_HOME/etc/shcluster/apps/` folder and deploy the Splunk App for VMware app onto any member of your SHC.

   ```bash
   ./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>
   ```

6. Restart Splunk in each of the locations where you installed the app.
Learn More

♦ For an overview of search head clustering, see Search head clustering architecture in the "Splunk Enterprise Distributed Search Manual".
♦ See Deploy a search head cluster in the Splunk Enterprise Distributed Search Manual.
♦ See "Use the deployer to distribute apps and configuration updates" in the Splunk Enterprise Distributed Search Manual.
♦ See configure a complex deployment for more information on how to configure the Splunk App for VMware in a complex deployment.

Configure license

In order to use the Splunk App for VMware, you need a valid license. This VMware license is in addition to the license(s) you need to use your Splunk platform deployment. The license works for both local and remote license master configurations. Your app license volume does not add indexing volume to your Splunk Enterprise license. If your VMware deployment is missing a valid license, you will receive a license violation notification.

To address this problem, follow these steps:

1. Contact Splunk Sales. Tell them how much data per day you plan to use with the Splunk App for VMware.
2. Once you have been provided an invoice, pay the designated amount. Splunk will send you a license key.
3. Once you receive the license key, install the license into the Splunk Enterprise server that hosts your licenses.

Note: You can install the paid license at any time during the 90 day trial period but you must install it in order to view your VMware app data once the trial license expires.

Add a new license

To add a new license:

1. Navigate to Settings > Licensing.
2. Click Add license.
3. Either click **Choose file** and browse for your license file and select it, or click **copy & paste the license XML directly...** and paste the text of your license file into the provided field. **Note:** If you install a Dev/Test license with an Enterprise license, the Enterprise license file will be replaced.

4. Click **Install.** If this is the first Enterprise license that you are installing, you must restart Splunk Enterprise. Your license is installed.

**App License Status**

The App License Status dashboard of the Splunk App for VMware displays data on the status of your Splunk App for VMware license. Use this dashboard to see:

- The status of your license
- Monitor messages
- Days remaining until your app license expires
- Total data usage in GB

Users will be routed to the **App License Status** page if a functional license is not detected.

Use the **Refresh** button to check the status of your license.

Use the **App Data Volume** page to monitor license usage. See the App Data Volume section of this manual.

**Frequently Asked Questions**

*How do I know what size license I will need?*

When you contact Splunk Sales, they can help you determine the correct license quota based on the number of servers you have in your environment and what data you want to index.

**Which server hosts the licenses?**

The Splunk Enterprise server that hosts your Splunk licenses (known as the **license master**) depends on how you have configured the central Splunk App for VMware instance.
In many cases, Splunk Enterprise holds licenses on the server that performs indexing for the Splunk App for VMware. Depending on how you configured the central Splunk App for VMware instance, the master license server might be on a different Splunk Enterprise instance within the deployment.

**What happens if I don’t have a Splunk App for VMware license?**

The Splunk App for VMware requires that you have a license to view your VMware data. If you don't have a license, use the instructions above to get a valid license key from Splunk Support.

**What happens if I violate my license?**

If you violate your Splunk App for VMware license, the app gives you a warning that you have exceeded your daily indexing limit. If you continue to violate your license within a 30-day period, the license violation will disable all VMware app pages except for the following admin management pages:

- App Data Volume
- App License Status
- App Install Health
- Configured Thresholds

Data collection will continue as normal. License violations do not have a reset feature. Users will need to wait until midnight of the next day, or contact Sales or Support to receive a temporary trial license.

If your deployment has been disabled by a license violation, contact Splunk Support for assistance in lifting the restriction.

Note: This also happens if the Splunk App for VMware cannot find a valid license.

**Does the Splunk App for VMware change the amount of data I can index in Splunk Enterprise?**

No. It does not increase or decrease the amount of indexing capacity on your Splunk Enterprise servers.
Assign user roles for Splunk App for VMware

Splunk App for VMware creates roles called `splunk_vmware_user` and `splunk_vmware_admin` within the Splunk platform. Assign these roles to existing users or groups of users to grant them access to the Splunk App for VMware and the Splunk Add-on for VMware. Make sure that you add these roles to the admin user of your Splunk platform instance.

1. Log in to Splunk Web on the search head using the IP address and port number of the search head: https://<ipaddress>:8000/. Use https (not http) to access the dashboards.
2. From the Apps menu, select **Splunk App for VMware**.
3. Provide `admin_all_objects` capability to the `splunk_vmware_admin` role. Go to the Settings > Access controls > Roles > `splunk_vmware_admin` and add `admin_all_objects` capability and click Save.
4. Accept the default settings, and click Save.
5. To assign user roles for the Splunk App for VMware and the Splunk Add-on for VMware, select Settings > Access controls > Users.
6. Assign both the `splunk_vmware_admin` and the `splunk_vmware_user` roles to the admin user of your Splunk Enterprise instance. Users with the administrator role can configure data collection or thresholds for Splunk App for VMware.
7. Assign the `splunk_vmware_user` role to each user or user group that requires access Splunk App for VMware.

Deploy the Splunk OVA for VMware to create a Data Collection Node

See the Install the Splunk OVA for VMware section of the Splunk OVA for VMware and NetApp documentation for information on creating and deploying the Splunk OVA for VMware and NetApp.

Notes

- Download the Splunk OVA for VMware from Splunkbase.
- Set up forwarding to the port on which the Splunk indexer(s) is configured to receive data. See "Enable forwarding on a Splunk Enterprise instance" in the Forwarding Data manual.
Configure the data collection node and system settings

See Configure the Splunk OVA for VMWare in the Splunk OVA for VMWare and NetApp documentation.

Notes

- In a Search Head Clustering (SHC) deployment, the DCN Scheduler must not be deployed on any individual Search Head in the SHC. The DCN Scheduler must be deployed on a dedicated search head.

- See Deploy OVA to create a Data Collection Node for DCN installation.

Configure Splunk App for VMware to collect data from vCenter Server

Configure a Data Collection Node

The Collection Configuration dashboard, on the search head, manages the Data Collection Nodes (DCNs). 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.

Register a DCN with the scheduler

1. Log in to Splunk Web on the search head as admin.
2. From the App menu, select VMware.
3. From the Settings menu select Collection Configuration, and click +.
4. Enter the settings for the data collection node, and click Save. See the Data Collection Node configuration settings table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Forwarder URI</td>
<td>The address or port of the DCN. For example, https://&lt;host_name_or_ip_address_of_DCN&gt;:8089.</td>
</tr>
<tr>
<td>Splunk Forwarder Username</td>
<td>admin.</td>
</tr>
</tbody>
</table>
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.

## Configure vCenter Server

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

1. On the Collection Configuration dashboard, in the Virtual Centers panel, click +.
2. Enter the settings for the vCenter Server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Center FQDN</td>
<td>The fully-qualified domain name for the vCenter server. For example, test-vcenter100.example.com</td>
</tr>
<tr>
<td>VC Username</td>
<td>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.</td>
</tr>
<tr>
<td>VC Password</td>
<td>The password that you configured in vCenter Server for Splunk Enterprise.</td>
</tr>
</tbody>
</table>

3. For the initial installation, pull 20 or fewer hosts. If the vCenter Server manages other servers, make sure that Collect form all hosts and whitelist-specific hosts are not selected.
4. Click Save.
5. Verify that each of the vCenter Server entries displays a green check.
6. 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.

Collect VMware vCenter Server Linux Appliance log data

Use Splunk App for VMware with the Splunk Add-on for VMware to collect logs from the VMware vCenter Server Linux Appliance. The Splunk Add-on for VMware stores VMware vCenter Server Linux 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.
- You do not need to collect log data from a VMware vCenter Server Linux Appliance in order to see a working version of the Splunk App for VMware.

Export vCenter logs to an external system

1. Enable the VMware vCenter Server Application 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 the "Create NFS Datastore in the vSphere Client" in the VMware vSphere documentation.
2. On the system on which you have installed the Splunk Enterprise forwarder, install Splunk_TA_vCenter.
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 tomcat configuration files, edit the following stanzas in the `props.conf` file:
   
   a. Copy the
      
      `$SPLUNK_HOME/etc/Splunk_TA_vCenter/default/props.conf` file,
then paste into the $SPLUNK_HOME/etc/Splunk_TA_vCenter/local folder.
5. 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. Install Splunk_TA_vCenter on the Splunk Enterprise forwarder.
   1. Get the Splunk_TA_vcenter-<version>-<build_number>.zip file from the download package and place it on vCenter.
   2. Unzip the Splunk App for VMware package.
      ```
      cd /opt/splunkforwarder
      Splunk_TA_vcenter-<version>-<build_number>.zip
      ```
   1. Verify that you extracted the Splunk_TA_vcenter/ in 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. Start your Splunk Universal Forwarder.
Troubleshoot

Troubleshoot Splunk App for VMware

1. Review the release notes to determine if the trouble you are experiencing is a known issue.
2. Consider enabling the troubleshooting logs on data collection nodes to facilitate root cause investigation. See Enable troubleshooting logs.
3. Review the following problems for advice on how to resolve them.

Problems to troubleshoot

Problem

- If you are getting "Problem editing the number of worker inputs on the remote node" error in splunk_for_vmware_setup.log
- If you are getting "could connect to splunkd but failed to auth check username and password" error in hydra_scheduler_ta_vmware_collection_scheduler_puff.log
- If you are getting "unable to retrieve the EAI _new descriptor for entity: configs/conf-hydra_metadata" error in splunkd.log
- On scheduler, if you are unable to update or validate the configurations on collection configuration page.

Cause

Splunk user of schedular and DCN does not have admin_all_objects capability added to the splunk_vmware_admin role.

Resolution

Follow the below steps on schedular and DCN.

1. Splunk user which is used to configure the collection configurations and the Splunk user of DCN which is used to configure the DCN must have splunk_vmware_admin role.
2. splunk_vmware_admin role should have admin_all_objects capabilities.
Problem

Splunk App for VMware does not seem able to make read-only API calls to vCenter Server systems.

Cause

You do not have the appropriate vCenter Server service login credentials for each vCenter Server.

Resolution

Obtain vCenter Server service login credentials for each vCenter server. See Permissions in vSphere.

Problem

$vpxd.stats.maxQueryMetrics$ error prevents data collection from vcenters.

Cause

As of version 6.0 VMware vCenter has added a limitation to the number of performance metrics collected by the $vpxd.stats.maxQueryMetrics$ function. The vCenter 6.0 maxQuerySize limit is 64 metrics per query. This 64 metric limit is calculated by multiplying the number of metrics queried by the number of entities (virtual machines) being queried. For example, querying 8 entities (virtual machines) for 10 metrics from each entity (virtual machine) equals a query size of 80.

Resolution

To adjust the maxQuerySize limit:

1. Navigate to the advanced settings of vCenter Server, or vCenter Server Appliance.
2. Edit the config.vpxd.stats.maxQueryMetrics key.

See the VMware documentation for more information.

Problem
You have configured vCenter Server 5.0 in Splunk App for VMware, but no data is coming in.

**Cause**

vCenter Server 5.0 and 5.1 are missing WSDL files that are required for Splunk App for VMware to make API calls to vCenter Server.

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

**Resolution**

Install 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.

**Problem**

The individual tests in the deployment section work, but the Splunk App for VMware main dashboard is empty.

**Cause**

This is typically caused by one of two issues:

- Time synchronization issues between the indexer, DCN, and vCenter Server
- Incorrect permissions assignments in Splunk Enterprise

**Resolution**

- Check for time gaps between the indexer, DCN, and vCenter Server. See validation topic for details. To adjust or disable the Network Time Protocol (NTP) on your DCN, see Designate NTP servers for a DCN.
- Make sure that you have assigned the correct roles to users of Splunk Enterprise.

<table>
<thead>
<tr>
<th>User</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin user</td>
<td>splunk_vmware_admin</td>
</tr>
<tr>
<td>all users of the Splunk App for VMware</td>
<td>splunk_vmware_user</td>
</tr>
</tbody>
</table>
User Role

Problem

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

Cause

This is 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.

Resolution

- In the Splunk for VMware App Settings page, verify the accuracy of the settings in the collection page.
- Verify that the admin password for each DCN is not set to changeme.
- 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.

Problem

Splunk App for VMware works for 60 days, then stops.

Cause

The 60-day trial license for Splunk App for VMware has expired.

Resolution

Configure the DCN to join your Splunk Enterprise license pool.

    splunk edit licenser-localslave -master_uri https://myhost:8089

Problem
Splunk App for VMware seems to be collecting only partial data. Hosts are missing, and so on.

**Cause**

There are insufficient DCNs to handle the data volume coming from the ESXi environment.

**Resolution**

1. From the Settings page in Splunk App for VMware, review the list of hosts for each vCenter Server environment.
2. Verify that each DCN polls information for up to 40 ESXi hosts and 1,000 virtual machines (30/750 is recommended), based on the specifications for a 4 core DCN (the one configured with the OVA for VMware). Based on this sizing, a site that pulls information from 200 hypervisors and 5,000 VMs needs at least 5 DCNs.
3. Verify that 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. In the Splunk App for VMware configuration pane for the DCN, make sure that the number of worker processes is one fewer than the number of CPU cores assigned to the machine.

---

**Problem**

The DCNs are not delivering data to the Splunk Enterprise indexers.

**Cause**

If the DCNs are configured correctly, this problem is typically the result of a connectivity issue.

**Resolution**

* Make sure that the DCN has an IP address and can resolve DNS.
* Verify that no firewalls are preventing communication between the DCN and port 9997 on the indexers and that the Scheduler can connect to ports 8089 and 8008 on each DCN. On the search head, search `index=_internal host=DCN-hostname-here`.
In the Host Detail view of Splunk Enterprise version 6.0 or later, you see the following warning message:

Events may not be returned in sub-second order due to search memory limits configured in limits.conf:[search]:max_rawsize_perchunk. See search.log for more information.

Or, in search.log of Splunk Enterprise version 6.0 or later, you see the following warning message:

02-06-2014 15:47:04.353 ERROR databasePartitionPolicy - Max Raw Size Limit Exceeded
02-06-2014 15:47:04.467 WARN  CursoredSearch - Events may be returned not in exact sub-second order: M=1368 > N=1250, where M is the number of events read in the 1390841799th second, and N is max number of events to read in a single span. Note that N was scaled back because we exceeded limits.conf:[search]:max_rawsize_perchunk value=100000000

Cause

A bug: non-surppressed error message (SOLNVMW-3587)

Resolution

1. On indexers, add the following configuration in the limits.conf file in the $SPLUNK_HOME/etc/system/local directory:

```
limits.conf
[search]
max_rawsize_perchunk = 800000000
```

2. Restart the indexer.

3. Test to you if still see the error message in Splunk App for VMware Host Detail view.

Note that setting the value of max_rawsize_perchunk = 400000000 surppresses the warning message in the Host Detail view. However, in the search.log file, you will still see the following message:
Problem

Incomplete or no data coming from vCenters that are properly configured and connected to by a DCN. Data collection tasks are failing and/or connections between DCN and vCenter are closing before all data is transferred. This could be due to one of two issues.

- The collection tasks taking longer than the vCenter and app are expecting.
- Collection intervals are currently overloading your Data Collection Nodes (DCNs) and your vCenters.

Resolution

Change collection intervals in order to reduce the load on your Data Collection Nodes (DCNs) and your vCenters

1. Change the time interval for your host inventory job.
   1. On the instance where your scheduler is running, navigate to \etc\apps\Splunk_TA_vmware\default\.
   2. Open the ta_vmware_collection.conf file.
   3. Change hostinv_interval and hostinv_expiration from the 900 second default to a larger number (maximum 2700 seconds). Keep hostinv_interval and hostinv_expiration at the same number of seconds.
   4. Save your changes and exit.

2. Change the time interval for host performance data.
   1. On the instance where your scheduler is running, navigate to \etc\apps\Splunk_TA_vmware\local\.
   2. Open the ta_vmware_collection.conf file.
   3. Change hostvmperf_interval and hostvmperf_expiration from the 180 second default to a larger number (maximum 1200 seconds). Keep hostvmperf_interval and hostvmperf_expiration at the same number of seconds.
   4. Save your changes and exit.

3. Increase the timeout period in the vpxd file on your vCenter.
1. Open the vpxd.cfg file, located in `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\vpxd.cfg` file (\`C:\ProgramData\VMware\VMware VirtualCenter\vpxd.cfg` on Windows 2008) using a text editor.
2. Add the below information in the `<vpxd>` tags:

   ```xml
   <heartbeat>
   <notRespondingTimeout>180</notRespondingTimeout>
   </heartbeat>
   ```

1. Restart your VMware VirtualCenter Server service.

**Problem**

VMware App sets SSL for WebUI as Default

**Resolution**

Disable WebUI SSL in the Splunk App 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`

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

### Upgrade from tsidx namespaces to data model acceleration

Version 3.2.0 of the Splunk App for VMware replaces the use of tsidx namespaces with the use of data models and data model acceleration. Existing tsidx files will be not be deleted after the upgrade, and will not be utilized after the upgrade to version 3.2.0 of the Splunk App for VMware.

Previously (in versions 3.1.x and earlier), tsidx scheduling and storage was done on the search head. Starting in version 3.2.0, Data model acceleration is distributed and stored across your indexers. Spreading this task across your indexers instead of on your search head will promote more scalability across your installation.

See About data models to learn more.
Data model acceleration speeds up reporting for the entire set of attributes (fields) that you define in a data model. Data model acceleration creates summaries for the specific set of fields you and your Pivot users want to report on, accelerating the dataset represented by that collection of fields rather than a particular search against that dataset. It may take a few hours to create the data model acceleration depending on the amount of data that is historically indexed. Data that has not been accelerated yet (for example, live streaming data) will still be captured in queries by falling back to normal search for that data. Splunk Enterprise always process all summaries first, so accelerated data arrives faster.

See Accelerate data models to learn more.

Index storage size on your VMware indexes will remain unchanged with the implementation of data model acceleration. Previously (in versions 3.1.x and earlier), the age-based retention policy was 6 years, and the size-based retention policy was unlimited. Even if your raw data was deleted, tsidx data still existed, and performance and inventory charts were populated.

Starting in version 3.2.0, Data model acceleration has a **30-day retention policy**, and does not have an established size-based retention policy, and can, by default, take up an unlimited amount of disk space. Data model acceleration is dependent on your raw data. So if your raw data has been deleted, the accelerated data cannot be preserved, and your performance and inventory charts cannot be populated.

Click here to learn how to set size-based retention policies.

In versions 3.1.x and earlier, summarized data (tsidx) used approximately .42 MB per day for each virtual machine. In version 3.2.0, data model acceleration uses approximately .57MB per day for each virtual machine.

Your deployment’s Data Model acceleration properties are located in datamodels.conf on your indexers. See Data model acceleration configuration file reference in the Splunk App for VMware Configuration Guide to see the datamodels.conf default acceleration configuration.

**Map existing tsidx namespaces to data model nodes**

If you have built custom alerts, dashboards and/or reports using tsidx namespaces, use the table below to map your existing namespaces to nodes in the data models used by the VMware app.
### Namespace Data model Node name (not case sensitive)

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Data model</th>
<th>Node name (not case sensitive)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmw_perf_cpu_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.cpu.HostSystemCPU</td>
</tr>
<tr>
<td>vmw_perf_cpu_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.cpu.virtualmachineCPU</td>
</tr>
<tr>
<td>vmw_perf_datastore_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.datastore.virtualmachineDisk</td>
</tr>
<tr>
<td>vmw_perf_disk_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.disk.virtualmachineDisk</td>
</tr>
<tr>
<td>vmw_perf_mem_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.memory.virtualmachineDisk</td>
</tr>
<tr>
<td>vmw_perf_net_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.net.virtualmachineDisk</td>
</tr>
<tr>
<td>vmw_perf_power_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.power.virtualmachinePower</td>
</tr>
<tr>
<td>vmw_perf_resdisk_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.resdisk.virtualmachineDisk</td>
</tr>
<tr>
<td>vmw_perf_sys_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.sys.virtualmachineDisk</td>
</tr>
<tr>
<td>vmw_perf_rescpu_virtualmachine</td>
<td>VMWarePerformance</td>
<td>vmperformance.rescpu.virtualmachineCPU</td>
</tr>
<tr>
<td>vmw_perf_datastore_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.datastore.hostsystemDatastore</td>
</tr>
<tr>
<td>vmw_perf_disk_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.disk.HostSystemDisk</td>
</tr>
<tr>
<td>vmw_perf_hbr_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.hbr.hostsystemHbr</td>
</tr>
<tr>
<td>vmw_perf_mem_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.memory.HostSystemMemory</td>
</tr>
<tr>
<td>vmw_perf_net_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.net.hostsystemNet</td>
</tr>
<tr>
<td>vmw_perf_power_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.power.hostsystemPower</td>
</tr>
<tr>
<td>vmw_perf_resstorageadapter_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.resstorageadapter.HostSystemResStorageadapter</td>
</tr>
<tr>
<td>vmw_perf_storageadapter_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.storageadapter.HostSystemStorageadapter</td>
</tr>
<tr>
<td>vmw_perf_storagepath_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.storagepath.hostsystemStoragepath</td>
</tr>
<tr>
<td>vmw_perf_sys_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.sys.hostsystemSys</td>
</tr>
<tr>
<td>vmw_perf_rescpu_hostsystem</td>
<td>VMWarePerformance</td>
<td>vmperformance.rescpu.hostsystemResCPU</td>
</tr>
<tr>
<td>vmw_inv_datastore_virtualmachine</td>
<td>VMwareInventory</td>
<td>Inventory</td>
</tr>
</tbody>
</table>

### Manage deprecated namespace retention policies

The `$SPLUNK_HOME/etc/apps/SA-Utils/default/tsidx_retention.conf` file specifies the default retention policy for all deprecated namespaces.

To set a policy for each of the specific deprecated namespaces, create a `$SPLUNK_HOME/etc/apps/<add-on-name>/local/tsidx_retention.conf` file in each of the namespaces and configure the settings.

**Edit your retention.conf file:**

---

35
1. Edit the tsidx_retention.conf file to uncomment the deprecated namespaces that you want to use in the app.
2. Change the values associated with those namespaces.
   ♦ You can keep the default values for the deprecated namespaces or modify the settings to values that work in your environment.

The app also runs a script that cleans up the tsidx namespaces. How the files are cleaned up depends on the retention policy defined for the namespace in the $SPLUNK_HOME/etc/apps/SA-VMW-Performance/default/tsidx_retention.conf file.

TSIDX cleanup based on the file size cleans all tsidx files, but always leaves one file in that namespace. If you do not want to have one large tsidx file in the namespace, you can change the the maximum allowed size for the tsidx files.

**Change the the maximum allowed size for the tsidx files:**

1. Open the $SPLUNK_HOME/etc/system/local/limit.conf file.
2. Change the value of the parameter optimize_max_size_mb to specify a size limit for a single tsidx file.
3. Restart Splunk Enterprise.

**Remove SA-VMW-Licensecheck**

Splunk App for VMware 3.1.2 and earlier includes the SA-VMW-Licensecheck package. Refer to the Installation Guide for instructions on how to remove this package to avoid benign licensing error messages.

**Charts that only use summarized data**

Versions 3.2.0 and above of the Splunk App for VMware and versions 2.1.0 and above of the Splunk App for NetApp DATA ONTAP use data model acceleration to gather performance and inventory data. This means that if your data collection is not accelerated, some charts and tables will not be populated.

Use the table below to see which charts and panels use only summarized data.

**Dashboards using only summarized data**

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Path</th>
<th>Chart/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Detail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboard</td>
<td>Path</td>
<td>Chart/Table/Panel</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>VMWare &gt; Proactive Monitoring &gt; Entity Views &gt; Cluster Detail</td>
<td>Warning panel (Visible only when Cluster is in Warning or Critical state)</td>
<td>Warning panel 1 (Visible only when Cluster is in Warning or Critical state)</td>
</tr>
<tr>
<td>Home Proactive Monitoring</td>
<td>VMWare &gt; Home Proactive Monitoring</td>
<td>Virtual Machine Health - all gauges</td>
</tr>
<tr>
<td>Performance of Hosts and VMs</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Performance of Hosts and VMs</td>
<td>Timechart</td>
</tr>
<tr>
<td>Capacity Planning (Hosts)</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Capacity Planning (Hosts)</td>
<td>Table - Host Performance</td>
</tr>
<tr>
<td>Capacity Planning Cluster</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Capacity Planning Cluster</td>
<td>Table - Cluster Performance</td>
</tr>
<tr>
<td>Capacity Forecasting</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Capacity Forecasting</td>
<td>CPU Usage Prediction Over Time (%)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disk Usage Prediction Over Time (KBs/sec)</td>
</tr>
<tr>
<td>Capacity Planning for Clusters - CPU Headroom</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Capacity Planning for Clusters - CPU Headroom</td>
<td>Capacity statistics for Selected Cluster in the last 24 hours</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM's powered on in Selected Cluster in the last 24 hours</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Path</td>
<td>Chart/Table/Panel</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Capacity Planning for Clusters - Memory Headroom</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Capacity Planning for Clusters - Memory Headroom</td>
<td>Powered on VMs memory usage in the cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Currently used GB and Total Capacity over time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capacity statistics for Crest Cluster Cluster</td>
</tr>
<tr>
<td>Host System Detail</td>
<td>VMWare &gt; Proactive Monitoring &gt; Entity Views &gt; Host System Detail</td>
<td>Warning panel (Visible only when Host is in Warning or Critical state)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Drop Down used for Timechart</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timechart</td>
</tr>
<tr>
<td>Virtual Machine Detail</td>
<td>VMWare &gt; Proactive Monitoring &gt; Entity Views &gt; Virtual Machine Detail</td>
<td>Drop Down used for Timechart</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timechart</td>
</tr>
<tr>
<td>Virtual Machine Snapshots</td>
<td>VMWare &gt; Performance and Capacity Planning &gt; Virtual Machine Snapshots</td>
<td>Snapshots present on VM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Displays timechart when clicked on any row of table - Snapshots present on VM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timechart-Snapshot space used on disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timechart- Number of Snapshots on datastore</td>
</tr>
<tr>
<td>Proactive Monitoring</td>
<td>VMWare &gt; Proactive Monitoring &gt; Proactive Monitoring</td>
<td>On chart pin board Graph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vCenter Detail Chart</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluster Detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host Chart</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM Chart</td>
</tr>
</tbody>
</table>

Reports using only summarized data

<table>
<thead>
<tr>
<th>Panel/Chart</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average CPU Utilization</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Average CPU Utilization</td>
</tr>
<tr>
<td>Panel/Chart</td>
<td>Path</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Average Memory Provisioning</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Average Memory Provisioning</td>
</tr>
<tr>
<td>Average VM CPU Ready</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Average VM CPU Ready</td>
</tr>
<tr>
<td>Snapshots older than 14 days</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Snapshots older than 14 days</td>
</tr>
<tr>
<td>Max Disk Latency per VM</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Max Disk Latency per VM</td>
</tr>
<tr>
<td>Critical CPU Ready</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Critical CPU Ready</td>
</tr>
<tr>
<td>Critical CPU Usage</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Critical CPU Usage</td>
</tr>
<tr>
<td>Memory Utilization by Cluster</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Memory Utilization by Cluster</td>
</tr>
<tr>
<td>Critical Disk Usage</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Critical Disk Usage</td>
</tr>
<tr>
<td>Top Hosts with Ballooning</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Top Hosts with Ballooning</td>
</tr>
<tr>
<td>CPU Usage by Cluster</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; CPU Usage by Cluster</td>
</tr>
<tr>
<td>CPU Usage by VC</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; CPU Usage by VC</td>
</tr>
<tr>
<td>CPU Ready by VC</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; CPU Ready by VC</td>
</tr>
<tr>
<td>Memory Usage by VC</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Memory Usage by VC</td>
</tr>
<tr>
<td>Memory Ballooning by VC</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Memory Ballooning by VC</td>
</tr>
<tr>
<td>Memory Swapped by VC</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Memory Swapped by VC</td>
</tr>
<tr>
<td>Virtual Machine - Count by Disk Usage Severity</td>
<td>VMWare &gt; Knowledge Objects &gt; Reports &gt; Virtual Machine - Count by Disk Usage Severity</td>
</tr>
</tbody>
</table>
Panel/Chart | Path
---|---
Virtual Machine - Count by Memory Usage Severity | VMWare > Knowledge Objects > Reports > Virtual Machine - Count by Memory Usage Severity

To identify whether your data collection has been accelerated:

1. Navigate to the bottom of any chart panel, and click on the search icon to open a search string in a search view.
2. Look for "summariesonly=true", and replace it with "summariesonly=false", then run the search. If your timechart begins to populate, then your data collection has been accelerated.
3. Navigate to your data model settings and check progress of your data model acceleration.

**Set Splunk App for VMware trial license to work with remote license master**

If you install Splunk App for VMware in an environment that utilizes a remote server to manage your Splunk Enterprise license, you must set the app’s trial license to work with remote license master.

1. If you have not already done so, add a valid Splunk Enterprise license on the remote server that is acting as the license master. Refer to the Install a License topic for details.

2. On the local search head, navigate to Settings > Licensing, then click Change to slave to instruct the search head to point it to the remote server that is your license master. Refer to the Configure a slave license topic for details.

3. On the local search head, download and install Splunk App for VMware. Refer to the Download and install Splunk App for VMware topic for details.

4. Configure the app by following the steps in the App configuration wizard, then click Start Scheduler. For more information on how to configure a basic installation of the app, follow all the steps in the Install and deploy Splunk App for VMware chapter in the Installation Guide.

5. In Splunk App for VMWare, navigate to Settings > App License Status, then click Fix.
6. Enter your administrator credentials for your remote license master, then click **Apply Demo License**.

7. In the app, confirm that the App License Status indicates that the license is valid. It indicates an infinite number of days left but this is a known issue(SOLNVMW-3874). The actual number of days left in the trial license is 60.

8. Access the remote server that is acting as your license master. Navigate to Settings > Licensing to view the now valid App VMWare Download Trial license. It indicates approximately 60 days of validity but this is a known issue. The actual number of days left in the trial license is 60.
Upgrade Splunk App for VMware

Upgrade to Splunk App for VMware 3.4.4

Step 1: Download the files from Splunkbase

1. Download the Splunk App for VMware version 3.4.4 from Splunkbase to a location in your environment.
2. Download the Splunk Add-on for for VMware version 3.4.4 from Splunkbase to a location in your environment.
3. Download the Splunk OVA for VMware version 3.4.4 from Splunkbase to a location in your environment.

Step 2: Upgrade scheduler

Note: Make sure splunk_vmware_admin role has admin_all_objects capability.

1. Stop your Scheduler. You can do this by stopping the Splunk platform on your Splunk search head, or you can stop the scheduler in the Collection Configuration page of your deployment.
2. Overwrite splunk_TA_vmware, SA-Hydra and SA-VMNetAppUtils on your scheduler with new versions.
4. (Optional) If you are using your scheduler to collect data and want to keep the Splunk App for VMware running, then install and upgrade all app components.

Step 3: Upgrade forwarder (DCN)

Note: Make sure splunk_vmware_admin role has admin_all_objects capability.

1. Verify that your DCN components are the same as the components on your vCenter.
2. (Optional) If your DCN is on version 6.2.x or earlier, upgrade your DCN's Splunk platform to version 7.0.0 and higher.
3. Overwrite versions of Splunk_TA_vmware, SA-Hydra, SA-VMNetAppUtils and Splunk_TA_esxilogs on each data collection node with new versions.

**Step 4: Upgrade indexer**

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.
4. Push configuration bundle from cluster master node.

**Step 5: Upgrade search head**

Note: Make sure splunk_vmware_admin role has admin_all_objects capability.

**For search head cluster deployments**

1. Upgrade all the components on search head deployer. Components are located in etc/apps.
2. Copy the local folder from etc/apps/Splunk_TA_vmware from Search head to etc/shcluster/apps/TA-VMW-FieldExtractions on deployer.
3. Delete Splunk_TA_vmware from etc/shcluster/apps/ on your deployer.
4. Delete savedsearches.conf and tsidx_retention.conf from etc/shcluster/apps/SA-VMW-Performance/default/ on your deployer before applying the upgrade bundle.
5. Push app bundle from deployer. The deployer will restart all the search head cluster members after the upgrade is applied. If deployer does not restart the search head cluster members, perform a rolling restart.

**For dedicated search head deployments**

1. Upgrade all the components on Search head. Components are located in etc/apps.
2. Copy the local folder from Splunk_TA_vmware to TA-VMW-FieldExtractions from etc/apps on Search head.
3. Delete Splunk_TA_vmware from etc/apps/.
4. Delete savedsearches.conf and tsidx_retention.conf from etc/apps/SA-VMW-Performance/default/ on your Search head.
5. Splunk restart on Search head.

Step 6: Upgrade the forwarder on your vCenter server(s) This applies only to Windows-based vCenter servers - not vCSA.

1. Stop your Splunk forwarder.
2. On your vCenter server, navigate to `splunkforwarder/etc/apps`, and overwrite `Splunk_TA_vcenter`.
3. Delete your `local` directory.
4. Copy `inputs.conf` to `local` and enable stanza as per the vCenter server in this environment.
5. Confirm under `etc/system/local/output.conf`, server entries to forward vclogs are present.
6. Restart your forwarder.

Note: If you forward logs directly to Splunk indexes, or use an intermediate syslog forwarder, you do not need to set the inputs for vCenter logs.

Step 7: Start the scheduler

1. Navigate to the **Collection Configuration** page of the Splunk Add-on for VMware on your scheduler.
2. Start your scheduler.

*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
5. 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.