Splunk® App for Infrastructure
Install and Upgrade Splunk App for Infrastructure 2.1.0
Generated: 5/29/2020 4:50 am
# Table of Contents

## Introduction
- About the Splunk App for Infrastructure
- Licensing the Splunk App for Infrastructure
- Share data in Splunk App for Infrastructure

## Install SAI
- System requirements for Splunk App for Infrastructure
- SAI compatibility with related apps and add-ons
- Install the Splunk App for Infrastructure in a single-instance deployment
- Install the Splunk App for Infrastructure in a distributed deployment
- Install the Splunk App for Infrastructure in a Splunk Cloud deployment

## Upgrade SAI
- Upgrade to a new version of Splunk App for Infrastructure
- Upgrade to a new version of Splunk App for Infrastructure that's monitoring Windows systems
- Migrate to the new entity schema

## Install VMware data collection components
- VMware data collection planning and requirements
- Install VMware data collection add-ons and dependencies
- Deploy a Data Collection Node
- Deploy a Data Collection Scheduler

## Upgrade VMware data collection components
- Upgrade VMware data collection components
- Update a Data Collection Node after migrating Python versions
Introduction

About the Splunk App for Infrastructure

The Splunk App for Infrastructure (SAI) provides insight into the performance of Linux servers, Microsoft Windows servers, Amazon EC2, ELB and EBS instances, Kubernetes clusters, OpenShift clusters, Docker containers, and VMware vCenter Servers. SAI utilizes metrics for performance monitoring, and log data for deep understanding and troubleshooting of your server infrastructure.

Where to start

If you are using SAI with Splunk IT Service Intelligence (ITSI), see the ITSI Integrate the Splunk App for Infrastructure with ITSI guide.

For instructions on how to install and set up SAI in a single-instance or distributed deployment environment, see the Before you install and the Installation sections in this guide.

For instructions on how to administer SAI, including including adding data, advanced data collection tasks, creating alerts, configuring notifications, managing users and roles, and troubleshooting, see Administer Splunk App for Infrastructure.

For instructions on how to use an already configured instance of Splunk App for Infrastructure, see Use Splunk App for Infrastructure.

For information about new features, fixed issues, and known issues in this version of SAI, see Release Notes for Splunk App for Infrastructure.

Licensing the Splunk App for Infrastructure

The Splunk App for Infrastructure (SAI) uses ingestion based licensing that applies to your current Splunk Enterprise license. No additional license is required for SAI.

For more information, contact your Splunk sales representative.

Share data in Splunk App for Infrastructure

When the Splunk App for Infrastructure (SAI) is deployed on Splunk Enterprise, the Splunk platform sends data to Splunk Inc. ("Splunk"), and uses such data in accordance with the choices you made at the platform level. For information about how to opt in or out, and how the data is collected, stored, and governed, see Share data in Splunk Enterprise.

What data is collected

SAI collects the following additional basic usage information.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app.session.deployment.type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>app.session.monitoringInsightsConfigureTabLoad</td>
<td>Collects tab load time and usage for each integration to understand how the app is performing.</td>
<td>app: splunk_app_infrastructure deploymentType: INSIGHT page: investigate</td>
</tr>
<tr>
<td>app.session.monitoringInsightsPageLoad</td>
<td>Collects the page load time for each page visited to understand how the app is performing.</td>
<td>app: splunk_app_infrastructure loadTime: 7397.100000000137 metadata: { count: 328 currentTab: ENTITY selectedView: LIST_VIEW isInitialAppMount: true } mode: production page: SiiInvestigatePage</td>
</tr>
<tr>
<td>app.session.sai_ui_errors</td>
<td>Collects the error stacktrace associated with a page crash to understand why the app crashed.</td>
<td>app: splunk_app_infrastructure componentStack: in Connect(ConfigurePageContentsContainer) in Profiler (created by PageLoadProfiler) in PageLoadProfiler in ErrorBoundary (created by ErrorBoundarySai) in ErrorBoundarySai in Provider error: Cannot read property 'loadUserRoles' of undefined mode: test page: configure</td>
</tr>
<tr>
<td>app.sii.alertDefinitions</td>
<td>Collects the hashed alert title, alert metric, and alert aggregation model to understand usage around alert creation.</td>
<td>alertAggregationMethod: Avg alertMetricName: cpu.idle hashedAlertTitle: af62ee3e8d96d58199f28ec9aa7a1d</td>
</tr>
<tr>
<td>app.sii.appVersion</td>
<td>Collects the version of the app to understand new version adoption and usage.</td>
<td>appName: Splunk App for Infrastructure appVersion: 2.0.0</td>
</tr>
<tr>
<td>app.sii.backendPerformance</td>
<td>Collects method and process names and process names and method: discover_entities</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>app.sii.groupDefinitions</td>
<td>Collects the title, dimension key, and dimension value used to create each group to track the number of groups you create. The title and dimension value is always hashed, and the dimension key is hashed if you created it.</td>
<td>dimensionValue: mnjnkcxzjkkjk2389 &lt;br&gt; dimensionKey: dslkjkadofiuoo3489589 &lt;br&gt; groupTitle: kjhdsfhk453465D</td>
</tr>
<tr>
<td>app.sii.osType</td>
<td>Collects a count of hashed OS names that collectd forwards to understand the diversity of entity types.</td>
<td>osCount: 43 &lt;br&gt; osName: shk98sjckduy3ba8&amp;ksd</td>
</tr>
</tbody>
</table>
Install SAI

System requirements for Splunk App for Infrastructure

Review the following requirements before you deploy Splunk App for Infrastructure (SAI).

Splunk platform version requirements

Except as modified by statements on this page, all Splunk Enterprise system requirements apply to SAI deployments. For more information, see System requirements for use of Splunk Enterprise on-premises.

These are the compatible Splunk platform versions:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Enterprise</td>
<td>• 7.2.x</td>
</tr>
<tr>
<td></td>
<td>• 7.3.x</td>
</tr>
<tr>
<td></td>
<td>• 8.0.x</td>
</tr>
<tr>
<td>Splunk Cloud</td>
<td>• 7.2.6</td>
</tr>
<tr>
<td></td>
<td>• 7.2.7</td>
</tr>
<tr>
<td></td>
<td>• 8.0.x</td>
</tr>
</tbody>
</table>

Splunk add-on support and requirements

SAI requires these add-ons:

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Add-on for Infrastructure</td>
<td>2.0.x</td>
<td>Handles index creation, props, and transforms. SAI and the Splunk Add-on for Infrastructure are not backward compatible. You must run the same version of the app and add-on.</td>
</tr>
</tbody>
</table>

SAI is compatible with these add-ons:

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Add-on for Amazon Web Services</td>
<td>5.0.x</td>
<td>If you want to collect data from AWS CloudWatch, use the Splunk Add-on for Amazon Web Services.</td>
</tr>
<tr>
<td>Splunk Add-on for Microsoft Windows</td>
<td>5.0.1, 6.0.0, 7.0.0, 8.0.0</td>
<td>If you are upgrading from an earlier version of SAI, update props for the Splunk Add-on for Infrastructure in props.conf on every indexer and Windows Performance Monitor (perfmon) stanzas in inputs.conf on every universal forwarder sending data from a Windows system. For more information, see Upgrade to a new version of Splunk App for Infrastructure that’s monitoring Windows systems.</td>
</tr>
<tr>
<td>Splunk VMware OVA for ITSI</td>
<td>1.0.0, 1.1.0, 1.1.1</td>
<td>SAI uses this OVA for VMware integrations. If you want to monitor VMware data, you have to have an ITSI license.</td>
</tr>
</tbody>
</table>

Python 3 migration with Splunk Enterprise

On January 1, 2020, the Python Software Foundation will no longer support Python version 2.x. Existing Python packages and tools will end support for Python 2, and new Python packages won’t support Python 2. To maintain compatibility with the many third party projects that use Python, Splunk will migrate Splunk Enterprise, supported Premium Solutions, and supported Splunkbase apps and add-ons to Python 3.7 compatibility.
Splunk Enterprise version 8.0.x supports the migration from Python 2 to Python 3 by including both the Python 2.7 and Python 3.7 runtimes. Splunk will remove the Python 2.7 runtime altogether in a future release. For more information about the Python 3 migration, see Python 3 migration with the Splunk platform.

If you upgrade to Splunk Enterprise version 8.0.x, you have to upgrade to SAI version 2.0.0 or later. All SAI versions prior to 2.0.0 are incompatible with Splunk Enterprise version 8.0.x, even if you use the Python 2.7 runtime in Splunk Enterprise version 8.0.x. To upgrade to Splunk Enterprise version 8.0.x, first upgrade to SAI version 2.0.0 or later.

Operating system support for data collection

SAI supports data collection from the following operating systems. For information about operating system support for installation, see Operating system support for installation.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Supported version for data collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux/Unix (x86_64 only)</td>
<td>• RHEL 6, 7, 8&lt;br&gt;• CentOS 6, 7, 8&lt;br&gt;• Debian 7, 8, 9, 10&lt;br&gt;• Ubuntu 14, 16, 18.04, 18.10, 19&lt;br&gt;• Fedora 25, 26, 27, 28, 29, 30&lt;br&gt;• Solaris 10, 11&lt;br&gt;• SUSE Enterprise 12.3, 12.4, 12.5, 15&lt;br&gt;• openSUSE 42.3, 15.0, 15.1&lt;br&gt;There's no support for 32-bit with the easy install script.</td>
</tr>
<tr>
<td>Windows</td>
<td>• Windows Server 2012, 2012 R2, 2016, 2019 x86 (64-bit)&lt;br&gt;• Windows 10, x86 (64-bit), x86 (32-bit)&lt;br&gt;There's no support for 32-bit with the easy install script.</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>• Mac OS X 10.11-10.14</td>
</tr>
</tbody>
</table>

Third-party requirements

If you are collecting metrics data from a *nix host, you must install collectd. SAI is compatible with these versions of collectd:

• 5.7.x
• 5.8.x
• 5.9.x
• 5.10.x

For more information, see About using collectd.
**Supported browsers**

SAI supports the following browsers.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>Latest</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Version 11</td>
</tr>
<tr>
<td></td>
<td>This isn't supported in compatibility mode.</td>
</tr>
<tr>
<td>Safari</td>
<td>Latest</td>
</tr>
<tr>
<td>Chrome</td>
<td>Latest</td>
</tr>
</tbody>
</table>

*Linux data collection requirements*

You must have administrator privileges to run the easy install script. You can run the script only on compatible operating systems. For more information, see Operating system support for data collection.

For Mac OS X systems, the `/usr/local/sbin` directory must exist on the system, and you must log in as a user who can write to the directory.

For AWS Linux AMIs, agent-based data collection is not available. For AWS monitoring, see Configure AWS Data Collection in the Administer Splunk App for Infrastructure guide.

You must have these dependencies available:

<table>
<thead>
<tr>
<th>Operating system type</th>
<th>Required dependencies</th>
</tr>
</thead>
</table>
| Linux                 | • wget  
|                       | • apt-get (Debian and Ubuntu)  
|                       | • yum (Redhat, CentOS, and Fedora)  
|                       | • zypper (SUSE and openSUSE))  
|                       | • Internet access (easy install script)  |
| Mac OS X              | • curl  
|                       | • Homebrew  
|                       | • Internet access (easy install script)  |

For more information about how the data collection works, see How the easy install script works in Splunk App for Infrastructure in the Administer Splunk App for Infrastructure guide.

**Windows data collection requirements**

You must have admin privileges to run the easy install script.

The Windows system must have the following dependencies available:
• powershell
• Internet access (easy install script)

For more information about how the data collection works, see How the data collection script works in Splunk App for Infrastructure in the Administer Splunk App for Infrastructure guide.

**Kubernetes data collection requirements**

You must have permission to run `kubectl` commands on the system that's running a Kubernetes cluster. You also must have access to each Kubernetes cluster you monitor in SAI.

SAI requires Splunk Connect for Kubernetes version 1.2.0 or 1.3.0 to collect Kubernetes data.

You must run the script on a Linux or Mac OS X system, and it must have the following dependencies available:

- `kubectl`
- `Helm`
- `wget`
- Internet access (easy install script)

**OpenShift data collection requirements**

You must install Helm on a local system that's running the OpenShift cluster. Do not install Helm on the cluster.

SAI requires Splunk Connect for Kubernetes version 1.2.0 or 1.3.0 to collect OpenShift data.

To configure data collection, you must have these dependencies on the system you use to configure data collection:

- OpenShift CLI tool
- `Helm`
- `wget`
- Internet access (easy install script)

**Docker (no orchestration) data collection requirements**

You can monitor Docker containers on a Linux or Mac OS X system that you did not deploy with an orchestration tool like Docker Swarm, Kubernetes, or OpenShift.

These are the Docker requirements:

- Docker version 1.18 and higher
- Docker API version 1.20 and higher

You must have these dependencies:

- `libyajl2`
- `apt-get` (Debian or Ubuntu)
- `yum` (CentOS, Redhat, or Fedora)
- `zypper` (SUSE or openSUSE)
- Internet access (easy install script)
VMware data collection requirements

To view the requirements for setting up VMware data collection, see VMware data collection planning and requirements in the Install and Upgrade Splunk App for Infrastructure guide.

SAI compatibility with related apps and add-ons

This table lists versions of Splunk App for Infrastructure (SAI) and their compatible versions of the following related products:

- **IT Service Intelligence (ITSI)** has a built-in integration with SAI. See Integrate the Splunk App for Infrastructure with ITSI.
- **Splunk Add-on for Infrastructure** handles index creation, props, and transforms. See About the Splunk Add-on for Infrastructure.
- **Splunk Add-on for AWS** lets you collect data from AWS CloudWatch. See About the Splunk Add-on for Amazon Web Services.
- **Splunk Add-on for Microsoft Windows** collects Windows performance data. See Splunk Add-on for Windows.
- **Splunk VMware OVA for ITSI** is used for VMware integrations. See About the Splunk VMware OVA for ITSI.

<table>
<thead>
<tr>
<th>Splunk App for Infrastructure</th>
<th>Splunk Enterprise</th>
<th>IT Service Intelligence</th>
<th>Splunk Add-on for Infrastructure</th>
<th>Splunk Add-on for AWS</th>
<th>Splunk Add-on for Microsoft Windows</th>
<th>Splunk VMware OVA for ITSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.0</td>
<td>Python 3: 8.0.x</td>
<td>4.5.x</td>
<td>2.0.x</td>
<td>5.0.0, 5.0.1</td>
<td>5.0.1, 6.0.0, 7.0.0, 8.0.0</td>
<td>1.0.0, 1.1.0, 1.1.1</td>
</tr>
<tr>
<td></td>
<td>Python 2: 7.2.x, 7.3.x, 8.0.x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0.0, 2.0.1, 2.0.2</td>
<td>Python 3: 8.0.x</td>
<td>4.4.x</td>
<td>2.0.x</td>
<td>5.0.0, 5.0.1</td>
<td>5.0.1, 6.0.0, 7.0.0, 8.0.0</td>
<td>1.0.0, 1.1.0, 1.1.1</td>
</tr>
<tr>
<td></td>
<td>Python 2: 7.2.x, 7.3.x, 8.0.x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4.0, 1.4.1</td>
<td>7.1.x, 7.2.x, 7.3.x</td>
<td>4.2.x, 4.3.x</td>
<td>1.4.0</td>
<td>4.5.0</td>
<td>5.0.1</td>
<td>N/A</td>
</tr>
<tr>
<td>1.3.0, 1.3.1</td>
<td>7.0.x, 7.1.x, 7.2.x</td>
<td>4.1.x, 4.2.x</td>
<td>1.3.0</td>
<td>4.5.0</td>
<td>Not compatible. See SAI is not compatible with the Splunk Add-on for Windows.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Install the Splunk App for Infrastructure in a single-instance deployment

The single-instance Splunk Enterprise deployment serves as both the search head and the indexer. Install the Splunk Add-on for Infrastructure on the same instance of Splunk Enterprise on which you install the Splunk App for Infrastructure (SAI). If you install the Splunk Add-on for AWS, also install it on the same instance.

If you want to integrate VMware vCenter Servers in SAI, you have to install additional components. For more information, see Install VMware data collection add-ons and dependencies.
Steps

Follow these steps to get started with SAI in a single-instance deployment. In addition to installing SAI, these steps show you how to install the Splunk Add-on for Infrastructure, install the Splunk Add-on for AWS, and configure the receiving port for your instance.

1. Install SAI

Follow these steps to install the app.

1. In Splunk Web, go to Apps > Find More Apps.
2. Search for Splunk App for Infrastructure.
3. Select Install and follow the prompt.
4. Restart Splunk Enterprise.

2. Install the Splunk Add-on for Infrastructure

Follow these steps to install the Splunk Add-on for Infrastructure. When you install the add-on, it creates the em.metrics, em.meta, and infra_alerts indexes. For more information about the source types and components that the add-on configures, see Source types and components for the Splunk Add-on for Infrastructure.

For more information, see Splunk Add-on for Infrastructure.

1. In Splunk Web, go to Apps > Find More Apps.
2. Search for Splunk Add-on for Infrastructure.
3. Select Install and follow the prompt.
4. Restart Splunk Enterprise.

3. (Optional) Install the Splunk Add-on for AWS

If you want to collect AWS Cloudwatch data from your AWS accounts, follow these steps to install the Splunk Add-on for AWS. Version 5.0.0 is supported.

For more information, see About the Splunk Add-on for Amazon Web Services.

1. In Splunk Web, go to Apps > Find More Apps.
2. Search for Splunk Add-on for AWS.
3. Select Install and follow the prompt.
4. Restart Splunk Enterprise.

3. Configure the receiving port

Enable receiving on the TCP port for logs and metrics data collection.

1. In Splunk Web, log in as an administrator.
2. Click Settings > Forwarding and receiving.
3. Click Configure receiving. If your Splunk Enterprise instance is not already listening on port 9997, or is not listening to another port you plan to use, click New Receiving Port. If you are already listening on port 9997, go to the next step.
4. Specify the TCP port you want the receiver to listen on (the receiving port, also known as the listening port). The recommended port is 9997. For example, if you enter 9997, the receiver listens for connections from
forwarders on port 9997. You can specify any unused port. You can use a tool like `netstat` to determine what ports are available on your system. Make sure the port you select is not in use by Splunk Web or splunkd.

5. Click Save. Splunk software starts listening for incoming data on the port you specified.

**Install the Splunk App for Infrastructure in a distributed deployment**

To complete this task, you must be an administrator familiar with clustered environments on Splunk Enterprise.

You can deploy the Splunk App for Infrastructure in your distributed deployment of Splunk Enterprise. To do so, you need to complete these steps:

- Install SAI on the search head tier.
- Install the Splunk Add-on for Infrastructure on the indexer tier.
- Enable the HTTP Event Collector (HEC) on the indexer tier.
- If you want to collect AWS data, deploy or configure a heavy forwarder to handle AWS data collection.

If you want to integrate VMware vCenter Servers in SAI, you have to install additional Splunk add-ons, and configure a Data Collection Scheduler (DCS) and Data Collection Node (DCN). For more information, see Install VMware data collection add-ons and dependencies.

After you complete these steps, start collecting data from systems to monitor in the app. You can run the easy install script, or set up data collection manually. For more information, see the Administer Splunk App for Infrastructure guide.

**What the distributed deployment looks like**

This diagram describes a distributed environment that is ingesting data from a Windows system, a Mac system, a Linux system, a heavy forwarder for AWS data collection, and a DCN and DCS for VMware data collection. Each system sends S2S traffic from a universal forwarder directly to an indexer cluster and HTTP traffic from collectd to a third-party load balancer. The load balancer forwards traffic to HECs in the indexer cluster.
Where to install the App and other dependencies

The following table describes the required locations for installing the Splunk App for Infrastructure and other dependencies in your distributed deployment environment.

If you want to collect VMware data, there are some additional components you have to install. For information about where to install VMware data collection components, see Where to install VMware data collection components. For information about installing the VMware data collection components, see Install VMware data collection add-ons and dependencies.

<table>
<thead>
<tr>
<th>Component</th>
<th>Search heads</th>
<th>Indexers</th>
<th>Heavy forwarder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk App for Infrastructure</td>
<td>Required</td>
<td>Required</td>
<td>Required*</td>
<td>*Only when you deploy a heavy forwarder for AWS data collection.</td>
</tr>
<tr>
<td>Splunk Add-on for Infrastructure</td>
<td>Required</td>
<td>Required</td>
<td>Required*</td>
<td>You must install the add-on on each indexer to provide props and transforms for data types. *Only when you deploy a heavy forwarder for AWS data collection or use a heavy forwarder as an intermediary before you send data to an indexer.</td>
</tr>
<tr>
<td>Splunk Add-on for Amazon Web Services</td>
<td>Required</td>
<td></td>
<td></td>
<td>You must install the add-on if you are collecting data from AWS. Version 5.0.0 is supported.</td>
</tr>
<tr>
<td>HTTP Event Collector</td>
<td>Required*</td>
<td></td>
<td></td>
<td>*If you are collecting metrics from a *nix host, this is required. Collectd, which collects metrics data from *nix hosts, sends data to a HEC.</td>
</tr>
<tr>
<td>TCP input</td>
<td>Required*</td>
<td></td>
<td></td>
<td>*If you are collecting *nix and Windows logs and Windows metrics, configure a TCP input. You need to configure a port to receive data from a universal forwarder.</td>
</tr>
</tbody>
</table>

Steps

Follow these steps to set up the Splunk App for Infrastructure in a distributed Splunk Enterprise deployment.

1. Install the Splunk App for Infrastructure on search heads

Install the Splunk App for Infrastructure on every search head in the cluster. For more details about this task, see Deploy a configuration bundle in the Splunk Enterprise Distributed Search manual.

Prerequisite
First, check that you satisfy the system requirements for the Splunk App for Infrastructure. For more, see System requirements for Splunk App for Infrastructure.

1. Download the Splunk App for Infrastructure from Splunkbase.
2. On the machine that runs the search head cluster's deployer, copy the Splunk_App_Infrastructure directory to the $SPLUNK_HOME/etc/shcluster/apps directory.
3. Push the Splunk App for Infrastructure to every search head in the cluster:

```
$SPLUNK_HOME/bin/splunk apply shcluster-bundle -target <any_cluster_member_mgmt_url:mgmt_port> -auth <username:passwd>
```
2. Install the Splunk Add-on for Infrastructure on indexers

Install the Splunk Add-on for Infrastructure on the indexers. When you install the add-on, it creates the `em_metrics` and `infra_alerts` indexes, and handles props and transforms for all data types. For more information about the source types and components that the add-on configures, see Source types and components for the Splunk Add-on for Infrastructure in the Use Splunk Add-on for Infrastructure manual.

For more information about installing the add-on across an indexer cluster, see Update common peer configurations and apps in the Managing Indexers and Clusters of Indexers guide.

1. Download the Splunk Add-on for Infrastructure from Splunkbase.
2. On the machine that runs the indexer cluster master node, copy the `Splunk_TA_Infrastructure` directory to the `$SPLUNK_HOME/etc/master-apps` directory.
3. Validate the bundle and check whether a restart is necessary:
   ```bash
   splunk validate cluster-bundle --check-restart
   ```
4. Apply the bundle to the indexer cluster:
   ```bash
   splunk apply cluster-bundle
   ```
5. To see how the cluster bundle push is going, run this command:
   ```bash
   splunk show cluster-bundle-status
   ```

3. Configure inputs.conf for the indexing tier

Enable receiving on the TCP port for logs and perform metrics for Windows data collection for every indexer in the cluster. To do this, open a receiving port for the indexing tier. For more information about opening a receiving port, see inputs.conf in the Splunk Enterprise Admin Manual.

If you are collecting metrics data from a *nix host, also configure an HEC token. When you configure an HEC token, set the source type to `em_metrics`, and specify the metrics index you want to use. By default, the metrics index is `em_metrics`. For more information about configuring an HEC token, see Create an Event Collector token in the Getting Data In guide.

1. On the machine that runs the indexer cluster master node, go to the `$SPLUNK_HOME/etc/system/local` directory.
2. open the inputs.conf file with a text editor.
3. Add a `splunktcp` stanza:
   ```bash
   [splunktcp://<port>]
   disabled = 0
   where <port> is the port that you want to use to receive data from your host machines. The recommended value is 9997.
   ```
   For more information about configuring inputs.conf, see inputs.conf in the Admin Manual.
4. If you are collecting metrics data from a *nix host, add an HEC token stanza:
   ```bash
   [http://<token_name>]
   disabled = 0
   index = em_metrics
   indexes = em_metrics
   sourcetype = em_metrics
   token = <string>
   where <token_name> is the name of the token and <string> is a unique identifier for the token value.
5. If you have not already enabled global HEC settings, enable HEC now in an `http` stanza:
   ```bash
   [http]
   ```
4. **Push the indexer cluster master node’s configuration bundle to the indexer cluster**

Push the Splunk_TA_Infrastructure directory and inputs.conf file to every indexer in the indexer cluster. For more information, see Update common peer configurations and apps.

On the machine that is running the indexer cluster master node, apply the configuration bundle to every indexer in the cluster:

```
$SPLUNK_HOME/bin/splunk apply cluster-bundle
```

5. **(Optional) Configure a heavy forwarder to collect AWS data**

If you haven't already deployed a heavy forwarder that can handle receiving AWS data, first deploy a heavy forwarder. For more information, see Deploy a heavy forwarder in the Splunk Enterprise Forwarding Data guide.

Install these apps and add-ons on the heavy forwarder:

- Splunk App for Infrastructure
- Splunk Add-on for Infrastructure
- Splunk Add-on for AWS

For information about installing apps and add-ons, see Where to get more apps and add-ons in the Splunk Enterprise Admin Manual.

5. **(Optional) Deploy a DCN and DCS**

You have to deploy a DCN and DCS to collect VMware data. Before you do this, confirm that your indexers have been set up properly. For information about configuring your deployment for VMware data collection, see Install VMware data collection add-ons and dependencies.

To deploy a DCN, see Deploy a Data Collection Node.

To deploy a DCS, see Deploy a Data Collection Scheduler.

6. **Configure data collection**

Configure data collection for the Splunk App for Infrastructure using the easy install script under the **Add Data** tab. You can collect data from Linux, Mac OS X, and Windows hosts, Kubernetes and OpenShift clusters, and VMware vCenter Servers.

The easy install script in the **Add Data** tab cannot set up data forwarding to multiple indexers or a load balancer. If you are sending data to multiple indexers or a load balancer, manually configure data collection.

For information about configuring data collection, see How to add data to Splunk App for Infrastructure in the **Administer Splunk App for Infrastructure** manual.

For more information on package source, install commands, and install locations for collectd and the collectd plug-in according to the supported operating system, see collectd package sources, install commands, and locations in the **Administer Splunk App for Infrastructure** manual.
Install the Splunk App for Infrastructure in a Splunk Cloud deployment

You must be a Splunk Cloud administrator to install and manage apps in your Splunk Cloud environment. To install an app on Splunk Cloud, contact your Splunk sales representative or Splunk Support. You will need Splunk Support to complete these tasks:

- Add the Splunk App for Infrastructure (SAI) to your Splunk Cloud environment.
- Add the Splunk Add-on for Infrastructure to your Splunk Cloud environment.
- Enable the HTTP Event Collector (HEC) in your Splunk Cloud environment.

If you want to collect VMware data, Splunk Support also has to complete these tasks:

- Install VMware data collection components.
- Confirm you have an ITSI license.

After Splunk Support installs the app and add-ons, and enables HEC for your cloud environment, configure your Splunk Cloud instance and hosts to send data to SAI.

You have to use the `sc_admin` user to make configuration changes.

What the cloud deployment looks like

Install a universal forwarder for metrics and logs collection on Windows systems. Install a universal forwarder for logs collection and `collectd` for metrics collection for *nix systems. You have to install universal forwarder credentials on every system you install a universal forwarder on. Data the universal forwarder collects is sent to the indexing tier in the cloud environment.

You must install `collectd` on *nix systems for metrics collection. `Collectd` sends data to an HEC in the indexing tier in the cloud environment.

If you plan to send VMware data to SAI, you have to deploy a Data Collection Node (DCN) and Data Collection Scheduler (DCS). For more information, see Install VMware data collection add-ons and dependencies.

If you plan to send AWS data to SAI, you have to deploy a heavy forwarder on a Windows or Linux system and install the Splunk Add-on for AWS, the Splunk Add-on for Infrastructure, and the universal forwarder credentials on it. To configure the heavy forwarder to send AWS data to SAI in the cloud environment, also install SAI on it.

This diagram describes a cloud environment that is ingesting data from a Windows system, a Mac system, a Linux system, and a heavy forwarder for AWS data collection.
Configure your cloud deployment for SAI

Follow these steps to set up your physical and cloud environment to start sending data to SAI.

1. **Add the power role to sc_admin users**

To fully configure and use SAI as an sc_admin user, ensure that all capabilities are assigned to each sc_admin user that has access to the cloud environment.

For more information about assigning the power capabilities to the sc_admin user, see sc_admin role permissions.

2. **Install and configure the data collection agents on each applicable system**

Do not run the easy install script or manually install data collection agents on a heavy forwarder that sends AWS data to SAI.

Use the easy install script to configure the data collection agents on each system that sends data to the cloud environment. For Windows systems, the easy install script installs and configures a universal forwarder. For *nix systems, the easy install script installs and configures a universal forwarder and collectd.

For information about the data collection script for each OS, see these topics in the *Administer Splunk App for Infrastructure* guide:

- Collect Windows metrics and logs with Splunk App for Infrastructure
- Collect Linux/Unix metrics and logs with Splunk App for Infrastructure
- Collect Mac OS X metrics and logs with Splunk App for Infrastructure

You can also manually set up the universal forwarder and collectd. For more information, see these topics in the *Administer Splunk App for Infrastructure* guide:
• Manually configure metrics and log collection for Windows on Splunk App for Infrastructure
• Manually configure log collection on a *nix entity for Splunk App for Infrastructure
• Manually configure metrics collection on a *nix entity for Splunk App for Infrastructure

When you are configuring data collection, use these port values so that your cloud stack receives data from your systems:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Machine</td>
<td>http-inputs-&lt;cloud_hostname&gt;.splunkcloud.com</td>
</tr>
<tr>
<td>HEC port</td>
<td>443</td>
</tr>
</tbody>
</table>

3. **Install universal forwarder credentials**

Follow this step for each system that is not already sending data to your cloud environment. Otherwise, skip this step.

You must install the universal forwarder credentials file on each system that sends data to your cloud environment. The universal forwarder credentials file contains a custom certificate for your Splunk Cloud deployment. The universal forwarder credentials are different from the credentials that you use to log into Splunk Cloud.

Before you install the universal forwarder credentials, remove `outputs.conf` on the universal forwarder that the script installed and configured.

If you have not already created a user for the universal forwarder, first create a user. To create a user, add credentials to a `user-seed.conf` file. For more information, see `user-seed.conf` in the Splunk Enterprise Admin Manual. If you modify a conf file, be sure to restart `splunkd` so your changes take effect.

By default, you must be the root user to make changes to the universal forwarder directory.

1. Log in to your Splunk Cloud homepage.
2. In the left sidebar, click **Universal Forwarder**.
3. Click **Download Universal Forwarder Credentials** to download the `splunkclouduf.spl` file.
4. From a command-line interface, go to the `$SPLUNK_HOME/bin` directory for your universal forwarder.
5. Run the following command:
   ```bash```
   ./splunk install app <full_path_to_splunkclouduf.spl> -auth <username>:<password>
   where `<username>:<password>` are the login credentials for an existing account on the universal forwarder.
   ```bash```
6. Restart the universal forwarder:
   ```bash```
   ./splunk restart

4. **Set up AWS data collection**

When deploying a heavy forwarder to collect AWS data for SAI, you have to set up only forwarding on it. You do not have to set up receiving.

1. If you plan to collect AWS data, install apps and add-ons on a **heavy forwarder**:
   1. Splunk App for Infrastructure
   2. Splunk Add-on for Infrastructure
   3. Splunk Add-on for AWS version 5.0.0
   4. universal forwarder credentials
2. Configure AWS data collection. For information, see Configure AWS data collection for Splunk App for Infrastructure.

For information about installing apps and add-ons, see Where to get more apps and add-ons in the Splunk Enterprise
For information about deploying a heavy forwarder, see Deploy a heavy forwarder in the Splunk Enterprise Forwarding Data guide.

4. Set up VMware data collection

To collect VMware data collection, you have to install and configure a Data Collection Node (DCN) and Data Collection Scheduler (DCS) outside of Splunk Cloud. To set up a DCN and DCS, see these topics:

- Deploy a Data Collection Node
- Deploy a Data Collection Scheduler

VMware data collection with Splunk Cloud requires that you configure a universal forwarder with universal forwarder credentials between the DCN and the Splunk Cloud indexer endpoint. Configure the DCN to forward data to the universal forwarder. The universal forwarder will then send data from the DCN to Splunk Cloud with the proper credentials. For more information, see Install universal forwarder credentials.

You can install the universal forwarder on the system that's running the DCN. For steps about deploying a universal forwarder, see Install a *nix universal forwarder in the Splunk Universal Forwarder Forwarder Manual.

For information about installing VMware data collection components, see Install VMware data collection add-ons and dependencies.

After you install the data collection components, set up VMware data collection. For more information, see Collect VMware vCenter Server metrics with Splunk App for Infrastructure in the Administer Splunk App for Infrastructure guide.
Upgrade SAI

Upgrade to a new version of Splunk App for Infrastructure

Integration with Splunk IT Service Intelligence (ITSI) is enabled by default. If you're upgrading ITSI while SAI is already installed in your environment, the SAI version is automatically upgraded to the most recent version.

When you upgrade to a new version of SAI, install the new package directly over your existing deployment in Splunk Enterprise.

Before you upgrade

Learn important information and tips about the upgrade process.

• If you're monitoring metrics for Windows systems, update Windows Performance Monitor (perfmon) stanzas in inputs.conf for the Splunk Add-on for Infrastructure and each universal forwarder on a Windows system. Version 1.4.0 introduced new perfmon stanzas that migrate perfmon inputs from a log-based format to a metrics-based format. If you're upgrading from a version earlier than version 1.4.0, you have to update inputs.conf on every universal forwarder and props.conf on every indexer. You won't receive perfmon data from Windows systems you're monitoring until you update inputs.conf and props.conf. For more information about updating perfmon stanzas, see Upgrade to a new version of Splunk App for Infrastructure that's monitoring Windows systems.
• If you're upgrading from version 1.2.0 or 1.2.1, remove the limits.conf file from the $SPLUNK_HOME/etc/apps/splunk_app_infrastructure/default directory.
• Review the release notes, known issues, and system requirements for the version you are upgrading to.
• Back up your existing deployment before you perform any upgrade.
   ♦ You can manage upgrade risk by using technology that lets you restore your installation and data to a state prior to the upgrade, whether that is external backups, disk or file system snapshots, or other means. When backing up your data, consider the $SPLUNK_HOME directory and any indexes outside of it.
• Downgrading SAI isn't supported.

Upgrade to new version of SAI

1. Before you upgrade, back up all of your files.
2. Obtain a new version of SAI. Go to Splunkbase.
3. Open a shell prompt on the host that has the instance that you want to upgrade.
4. Change to the $SPLUNK_HOME/bin directory.
5. Run the $SPLUNK_HOME/bin/splunk stop command to stop the instance.
6. Confirm that no other processes can automatically start SAI.
7. Install the package directly over your existing deployment. See Install the Splunk App for Infrastructure.
8. Run the $SPLUNK_HOME/bin/splunk start command, or go to the user interface and restart the application.

Upgrade to a new version of Splunk App for Infrastructure that's monitoring Windows systems

Splunk App for Infrastructure (SAI) version 1.4.0 changed Windows Performance (perfmon) inputs in inputs.conf and props in props.conf to migrate perfmon inputs from a log-based format to a metrics-based format in Splunk Enterprise.
SAI stores metrics in a metrics index rather than an events index.

When you upgrade to version 1.4.0, you must complete these actions:

- Update perfmon inputs in `inputs.conf` on every universal forwarder that's handling perfmon inputs.
- Update props in `props.conf` for the Splunk Add-on for Infrastructure.

You must use SAI version 1.4.0 with the Splunk Add-on for Infrastructure version 1.4.0. The app and add-on are not backward compatible. For example, you can’t run SAI version 1.3.1 with the Splunk Add-on for Infrastructure version 1.4.0.

Until you update Windows Performance Monitor (perfmon) inputs and props, you won’t collect Windows perfmon data from Windows systems you’re monitoring.

**What changed in version 1.4.0**

**inputs.conf:** Perfmon stanza names have changed, and each perfmon stanza now specifies a sourcetype.

**props.conf:** Perfmon prop names have changed.

The following changes are for the default perfmon inputs you can configure from the Add Data pages in the UI. If you are collecting other perfmon inputs, you have to update the inputs and props for those as well.

These are the new perfmon stanza names and source types in `inputs.conf`:

<table>
<thead>
<tr>
<th>Old perfmon stanza name</th>
<th>New perfmon stanza name</th>
<th>Source type</th>
</tr>
</thead>
<tbody>
<tr>
<td>[perfmon://CPU Load]</td>
<td>[perfmon://CPU]</td>
<td>PerfmonMetrics:CPU</td>
</tr>
<tr>
<td>[perfmon://Available Memory]</td>
<td>[perfmon://Memory]</td>
<td>PerfmonMetrics:Memory</td>
</tr>
<tr>
<td>[perfmon://System]</td>
<td>[perfmon://System]</td>
<td>PerfmonMetrics:System</td>
</tr>
<tr>
<td>[perfmon://Free Disk Space]</td>
<td>[perfmon://LogicalDisk]</td>
<td>PerfmonMetrics:LogicalDisk</td>
</tr>
</tbody>
</table>

These are the new perfmon prop names in `props.conf`:

<table>
<thead>
<tr>
<th>Old prop stanza name</th>
<th>New prop stanza name</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Perfmon:CPU]</td>
<td>[PerfmonMetrics:CPU]</td>
</tr>
<tr>
<td>[Perfmon:Memory]</td>
<td>[PerfmonMetrics:Memory]</td>
</tr>
<tr>
<td>[Perfmon:PhysicalDisk]</td>
<td>[PerfmonMetrics:PhysicalDisk]</td>
</tr>
<tr>
<td>[Perfmon:LogicalDisk]</td>
<td>[PerfmonMetrics:LogicalDisk]</td>
</tr>
<tr>
<td>[Perfmon:Network]</td>
<td>[PerfmonMetrics:Network]</td>
</tr>
<tr>
<td>[Perfmon:System]</td>
<td>[PerfmonMetrics:System]</td>
</tr>
<tr>
<td>[Perfmon:Process]</td>
<td>[PerfmonMetrics:Process]</td>
</tr>
</tbody>
</table>
**Example updated perfmon stanzas**

These perfmon stanzas are the default stanzas SAI adds to `inputs.conf` when you enable all default metrics on the **Add Data** page.

```plaintext
[perfmon://CPU]
counters = % C1 Time;% C2 Time;% Idle Time;% Processor Time;% User Time;% Privileged Time;% Reserved Time;% Interrupt Time
instances = *
interval = 30
object = Processor
index = em_metrics
_meta = os::"Microsoft Windows Server 2012 R2 Standard" os_version::6.3.9600 entity_type::Windows_Host
useEnglishOnly = true
sourcetype = PerfmonMetrics:CPU

[perfmon://PhysicalDisk]
counters = % Disk Read Time;% Disk Write Time
instances = *
interval = 30
object = PhysicalDisk
index = em_metrics
_meta = os::"Microsoft Windows Server 2012 R2 Standard" os_version::6.3.9600 entity_type::Windows_Host
useEnglishOnly = true
sourcetype = PerfmonMetrics:PhysicalDisk

[perfmon://Network]
counters = Bytes Received/sec;Bytes Sent/sec;Packets Received/sec;Packets Sent/sec;Packets ReceivedErrors;Packets Outbound Errors
instances = *
interval = 30
object = Network Interface
index = em_metrics
_meta = os::"Microsoft Windows Server 2012 R2 Standard" os_version::6.3.9600 entity_type::Windows_Host
useEnglishOnly = true
sourcetype = PerfmonMetrics:Network

[perfmon://Memory]
counters = Cache Bytes;% Committed Bytes In Use;Page Reads/sec;Pages Input/sec;Pages Output/sec;Committed Bytes;Available Bytes
interval = 30
object = Memory
index = em_metrics
_meta = os::"Microsoft Windows Server 2012 R2 Standard" os_version::6.3.9600 entity_type::Windows_Host
useEnglishOnly = true
sourcetype = PerfmonMetrics:Memory

[perfmon://System]
counters = Processor Queue Length;Threads
instances = *
interval = 30
object = System
index = em_metrics
_meta = os::"Microsoft Windows Server 2012 R2 Standard" os_version::6.3.9600 entity_type::Windows_Host
useEnglishOnly = true
sourcetype = PerfmonMetrics:System

[perfmon://Process]
counters = % Processor Time;% User Time;% Privileged Time
instances = *
```

21
Example updated perfmon prop stanzas

These props stanzas are the default stanzas SAI adds to props.conf when you enable all default metrics on the Add Data page.

[PerfmonMetrics:CPU]
TRANSFORMS-_value_for_perfmon_metrics_store = value_for_perfmon_metrics_store
TRANSFORMS-metric_name_for_perfmon_metrics_store = metric_name_for_perfmon_metrics_store
TRANSFORMS-object_for_perfmon_metrics_store = object_for_perfmon_metrics_store
TRANSFORMS-instance_for_perfmon_metrics_store = instance_for_perfmon_metrics_store
TRANSFORMS-collection_for_perfmon_metrics_store = collection_for_perfmon_metrics_store
EVAL-metric_type = "gauge"
SED CMD-remove-whitespace = s/ /_/g s/ / /g

[PerfmonMetrics:Memory]
TRANSFORMS-_value_for_perfmon_metrics_store = value_for_perfmon_metrics_store
TRANSFORMS-metric_name_for_perfmon_metrics_store = metric_name_for_perfmon_metrics_store
TRANSFORMS-object_for_perfmon_metrics_store = object_for_perfmon_metrics_store
TRANSFORMS-instance_for_perfmon_metrics_store = instance_for_perfmon_metrics_store
TRANSFORMS-collection_for_perfmon_metrics_store = collection_for_perfmon_metrics_store
EVAL-metric_type = "gauge"
SED CMD-remove-whitespace = s/ /_/g s/ / /g

[PerfmonMetrics:PhysicalDisk]
TRANSFORMS-_value_for_perfmon_metrics_store = value_for_perfmon_metrics_store
TRANSFORMS-metric_name_for_perfmon_metrics_store = metric_name_for_perfmon_metrics_store
TRANSFORMS-object_for_perfmon_metrics_store = object_for_perfmon_metrics_store
TRANSFORMS-instance_for_perfmon_metrics_store = instance_for_perfmon_metrics_store
TRANSFORMS-collection_for_perfmon_metrics_store = collection_for_perfmon_metrics_store
EVAL-metric_type = "gauge"
SED CMD-remove-whitespace = s/ /_/g s/ / /g

[PerfmonMetrics:LogicalDisk]
TRANSFORMS-_value_for_perfmon_metrics_store = value_for_perfmon_metrics_store
TRANSFORMS-metric_name_for_perfmon_metrics_store = metric_name_for_perfmon_metrics_store
TRANSFORMS-object_for_perfmon_metrics_store = object_for_perfmon_metrics_store
TRANSFORMS-instance_for_perfmon_metrics_store = instance_for_perfmon_metrics_store
TRANSFORMS-collection_for_perfmon_metrics_store = collection_for_perfmon_metrics_store
EVAL-metric_type = "gauge"
SED CMD-remove-whitespace = s/ /_/g s/ / /g

[PerfmonMetrics:Network]
TRANSFORMS-_value_for_perfmon_metrics_store = value_for_perfmon_metrics_store
TRANSFORMS-metric_name_for_perfmon_metrics_store = metric_name_for_perfmon_metrics_store
TRANSFORMS-object_for_perfmon_metrics_store = object_for_perfmon_metrics_store
TRANSFORMS-instance_for_perfmon_metrics_store = instance_for_perfmon_metrics_store
TRANSFORMS-collection_for_perfmon_metrics_store = collection_for_perfmon_metrics_store
EVAL-metric_type = "gauge"
SED CMD-remove-whitespace = s/ /_/g s/ / /g
Follow these steps to update perfmon props for the Splunk Add-on for Infrastructure and perfmon inputs for universal forwarders on Windows systems when you upgrade to version 1.4.0. If you’re using an indexer cluster master node to manage a distributed indexer deployment, use it to upgrade the Splunk Add-on for Infrastructure on each indexer.

For information about upgrading apps and add-ons, see Manage app and add-on objects in the Splunk Enterprise Admin Manual. If you’re running a distributed deployment, see Update common peer configurations and apps in the Splunk Enterprise Managing Indexers and Clusters of Indexers guide.

### 1. Upgrade SAI

Download SAI version 1.4.0 from Splunkbase and install the app package directly over existing app package as normal. You can do this manually, or from Splunk Web. There are no special steps to upgrade SAI if you're monitoring Windows systems. All of the work happens when you update the add-on and universal forwarders.

If you’re running a search head cluster, see Install the Splunk App for Infrastructure in a distributed deployment.

### 2. Upgrade the Splunk Add-on for Infrastructure

When you upgrade the Splunk Add-on for Infrastructure, remove the old perfmon props and transforms from `$SPLUNK_HOME/etc/apps/Splunk_TA_Infrastructure/default/props.conf` and `$SPLUNK_HOME/etc/apps/Splunk_TA_Infrastructure/default/transforms.conf`.

If you’re running a distributed deployment, see Install the Splunk App for Infrastructure in a distributed deployment for more information about installing the add-on in a distributed deployment.

1. On every instance running the Splunk Add-on for Infrastructure, move existing perfmon props from `$SPLUNK_HOME/etc/apps/Splunk_TA_Infrastructure/default/props.conf` to `$SPLUNK_HOME/etc/apps/Splunk_TA_Infrastructure/local/props.conf`. Doing this addresses a conf file precedence issue. These are the default stanzas SAI creates:
2. Upgrade the Splunk Add-on for Infrastructure to version 1.4.0.
3. Delete the props and transforms in $SPLUNK_HOME/etc/apps/Splunk_TA_Infrastructure/local/inputs.conf.

3. Update each Windows system you’re monitoring

You must update perfmon stanzas in inputs.conf on the universal forwarder on each Windows systems you’re monitoring. There are a few ways to do this:

- Run the updated easy install script from SAI version 1.4.0. For more information, see Collect Windows metrics and logs with Splunk App for Infrastructure in the Administer Splunk App for Infrastructure guide.
- Manually update perfmon stanzas on each universal forwarder. You must add the sourcetype field-value pair to each perfmon stanza in inputs.conf. For steps to do this, see Manually configure metrics and log collection for a Windows host for Splunk App for Infrastructure in the Administer Splunk App for Infrastructure guide.
- Use a third-party deployment server to update perfmon stanzas on each universal forwarder.

**Migrate to the new entity schema**

When you restart splunkd after upgrading to this version of the Splunk App for Infrastructure (SAI), the entity migration upgrade to the new entity schema automatically begins. The migration replaces collectors.conf with entity_classes.conf. The new conf file includes entity classes that are responsible for entity discovery under the new schema. Don't restart splunkd during the automatic migration process.

**What happens during the migration**

You don’t have to do anything for SAI to roll out the new entity schema. While SAI is migrating to the new schema, you can’t access any content in the app.

SAI carries out these actions during the migration to the new entity schema:

1. Logs everything to the _internal index.
2. Backs up all /local/ conf files and all local metadata files in metadata/local.meta.
3. Creates a tarball that contains all the backup files at $SPLUNK_HOME/etc/apps/splunk_app_infrastructure/migration_backup.
4. Disables all saved searches and modular inputs that belong to SAI.
5. Disables SAI’s REST API, and returns an HTTP 503 status code to all requests.

When the migration is complete, SAI enables all saved searches and modular inputs that belong to it, and enables its REST API.

**Delete the old key value store after a successful migration**

After the migration is successful, you can delete the key value store (KV store) for the previous entity schema.

**What to do if there’s a migration failure**

There are a couple things that could cause errors during the migration to the new entity schema:

- The new KV store for the new schema could take longer to initialize than SAI expects.
- Orphaned alerts fail the pre-migration process.
Install VMware data collection components

VMware data collection planning and requirements

Except as modified by statements on this page, all Splunk Enterprise system requirements apply to Splunk App for Infrastructure (SAI) deployments. For more information, see System requirements for use of Splunk Enterprise on-premises.

To install everything, see Install VMware data collection add-ons and dependencies. The SAI package doesn't contain any of the VMware data collection components. The Splunk IT Service Intelligence (ITSI) package contains all the VMware data collection components. The ITSI package contains the VMware data collection components because VMware data collection and monitoring in SAI requires an ITSI license.

If you're collecting VMware vCenter Server data and migrate Python versions, you have to update your Data Collection Node configuration. For more information, see Update a Data Collection Node after migrating Python versions.

License requirements

To configure VMware integrations, you need an ITSI license. Include an ITSI license on every Data Collection Scheduler (DCS) you use to integrate a VMware vCenter Server or Data Collection Node (DCN) in the Splunk App for Infrastructure (SAI) and every search head you use to monitor entities. For more information about ITSI licenses, see ITSI license requirements in the Install and Upgrade Splunk IT Service Intelligence guide.

Version compatibility

<table>
<thead>
<tr>
<th>Splunk Enterprise</th>
<th>VMware vSphere</th>
<th>VMware vCenter Server</th>
<th>VMware ESXi</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.x</td>
<td>6.0, 6.5, 6.7</td>
<td>6.0, 6.5, 6.7</td>
<td>6.0, 6.5, 6.7</td>
</tr>
<tr>
<td>7.3.x</td>
<td>6.0, 6.5, 6.7</td>
<td>6.0, 6.5, 6.7</td>
<td>6.0, 6.5, 6.7</td>
</tr>
<tr>
<td>8.0.x</td>
<td>6.0, 6.5, 6.7</td>
<td>6.0, 6.5, 6.7</td>
<td>6.0, 6.5, 6.7</td>
</tr>
</tbody>
</table>

Where to install VMware data collection components

This table provides the required install location for each VMware data collection component. You can forward data from a DCN either directly to an indexer or to an intermediary heavy forwarder. If you're running a single-instance deployment, the search head and indexer are on the same instance.

All of the VMware components are packaged in the `vmware_ta_itsi` parent directory of the Splunk IT Service Intelligence (ITSI) package you download from Splunkbase. You'll have to extract them from the directory and install them in the proper locations. For information about installing the components, see Install VMware data collection add-ons and dependencies.

<table>
<thead>
<tr>
<th>Component</th>
<th>Data Collection Scheduler (DCS)</th>
<th>Data Collection Node (DCN)</th>
<th>Indexer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk App for Infrastructure</td>
<td>X</td>
<td></td>
<td></td>
<td>Provides the UI for integrating VMware vCenter Servers and managing DCNs.</td>
</tr>
</tbody>
</table>
### Component Data Collection

<table>
<thead>
<tr>
<th>Component</th>
<th>Data Collection Scheduler (DCS)</th>
<th>Data Collection Node (DCN)</th>
<th>Indexer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Add-on for Infrastructure</td>
<td></td>
<td></td>
<td>X</td>
<td>Handles props and transforms needed for indexed extractions. Also includes index creation for SAI.</td>
</tr>
<tr>
<td>Splunk_TA_vmware</td>
<td>X</td>
<td>X*</td>
<td></td>
<td>Runs a Python-based API data collection engine and performs field extractions for VMware data.</td>
</tr>
<tr>
<td>*If you use the Splunk VMware OVA for ITSI to deploy a DCN, the DCN already has this component.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-Hydra</td>
<td>X</td>
<td>X*</td>
<td></td>
<td>Schedules data collection jobs on a scheduler, and runs worker processes on a DCN.</td>
</tr>
<tr>
<td>*If you use the Splunk VMware OVA for ITSI to deploy a DCN, the DCN already has this component.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-VMWIndex</td>
<td></td>
<td></td>
<td>X</td>
<td>Creates indexes that store VMware data.</td>
</tr>
<tr>
<td>Splunk_TA_esxilogs</td>
<td>X*</td>
<td></td>
<td>X</td>
<td>Handles log data collection from ESXi hosts.</td>
</tr>
<tr>
<td>*If you send syslog data to the DCN so the DCN forwards syslog data to the indexer tier.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk_TA_vcenter</td>
<td>X*</td>
<td></td>
<td>X</td>
<td>Handles vCenter data.</td>
</tr>
<tr>
<td>*If you send syslog data to the DCN so the DCN forwards syslog data to the indexer tier.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VMware indexes

VMWIndex creates these indexes.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmware-perf-metrics</td>
<td>Stores metrics data from a vCenter Server.</td>
</tr>
<tr>
<td>vmware-inv</td>
<td>Stores inventory data from a vCenter Server.</td>
</tr>
<tr>
<td>vmware-taskevent</td>
<td>Stores task and event data from a vCenter Server.</td>
</tr>
<tr>
<td>vmware-vclog</td>
<td>Stores vCenter Server log data.</td>
</tr>
<tr>
<td>vmware-esxilog</td>
<td>Stores ESXi host log data.</td>
</tr>
</tbody>
</table>

### Network port requirements

These are the ports you need to open to configure VMware data collection. The table includes the default Splunk ports. If you changed the Splunk ports, use those ports instead.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Collection Node requirements and limits

Each Data Collection Node (DCN) runs worker processes to collect VMware data from vCenter Servers. You can run \( N - 1 \) worker processes, where \( N \) is the number of the DCN's available CPU cores, up to 30 worker processes. The DCN requires physical CPU cores, and can't benefit from simultaneous multithreading (SMT). Each worker process can manage up to 250 virtual machines and 10 ESXi hosts.

If you deploy a DCN manually, the operating system you use has to be CentOS 6 or 7.

With `Splunk_TA_vmware` version 1.1.0, you can use an SSL certificate with an encrypted private key for Splunk Enterprise 7.3.3, 7.3.4, and 8.0.1.

These are the Splunk platform and operating system requirements to run a DCN if you don't use the Splunk VMware OVA for ITSI:

<table>
<thead>
<tr>
<th>Splunk Enterprise version</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.x</td>
<td>CentOS 6, 7</td>
</tr>
<tr>
<td>7.3.x</td>
<td>CentOS 6, 7</td>
</tr>
<tr>
<td>8.0.x</td>
<td>CentOS 6, 7</td>
</tr>
</tbody>
</table>

These are the minimum DCN hardware requirements:

<table>
<thead>
<tr>
<th>CPU</th>
<th>RAM</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-core CPU with a 2 GHz reservation</td>
<td>12 GB with a 1 GB reservation</td>
<td>12 GB storage capacity</td>
</tr>
</tbody>
</table>

These are the maximum ESXi hosts and virtual machines a single DCN can manage with the minimum DCN requirements:

<table>
<thead>
<tr>
<th>ESXi host</th>
<th>Virtual machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>1,750</td>
</tr>
</tbody>
</table>

Data Collection Scheduler requirements

A DCS schedules jobs and manages DCNs that collect data from vCenter Servers. Deploy a Data Collection Scheduler (DCS) on a search head in a standalone search head environment. If you're deploying VMware data collection in a distributed search head environment, deploy a DCS on a dedicated Splunk Enterprise instance. You don't have to configure forwarding or receiving on the DCS. To deploy a DCS, see [Deploy a Data Collection Scheduler](#).
Depending on your VMware environment, you may want to deploy more than one DCS. For more information, see Deployment considerations.

These are the requirements to run a Data Collection Scheduler (DCS):

<table>
<thead>
<tr>
<th>Splunk Enterprise version</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.x</td>
<td>CentOS 6, 7</td>
</tr>
<tr>
<td>7.3.x</td>
<td>CentOS 6, 7</td>
</tr>
<tr>
<td>8.0.x</td>
<td>CentOS 6, 7</td>
</tr>
</tbody>
</table>

**User account permissions**

When you integrate a VMware vCenter Server on a DCS, you have to provide credentials for a user account associated with the vCenter Server on the DCS. The DCS uses the user account credentials to detect ESXi servers in the vCenter Server, and to poll metrics, task, event, and inventory data.

The user account you provide on the DCS needs to have these permissions:

- Global.Diagnostics
- Global.Licenses
- Global.Settings
- Host.Configuration.Change SNMP settings
- Host.Configuration.Hyperthreading
- Host.Configuration.Memory configuration
- Host.Configuration.Network configuration
- Host.Configuration.Power
- Host.Configuration.Security profile and firewall
- Host.Configuration.Storage partition configuration
- Sessions.View and stop sessions
- System.Anonymous*
- System.Read*
- System.View*

*If you provide a user-defined role, it contains the System.Anonymous, System.Read, and System.View permissions even if you don’t associate them with the role manually.

**Daily data volumes**

These are rough estimates. Your daily volume may be more or less than the following volumes for each data type.

<table>
<thead>
<tr>
<th>Data type</th>
<th>Data volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server logs</td>
<td>15 MB per host per day.</td>
</tr>
<tr>
<td>ESXi logs</td>
<td>135-235 MB per host per day.</td>
</tr>
<tr>
<td>ESXi Host API</td>
<td>17 MB per host per day.</td>
</tr>
<tr>
<td>VM API</td>
<td>18 MB per VM per day.</td>
</tr>
</tbody>
</table>
Install VMware data collection add-ons and dependencies

Install the VMware data collection add-ons and dependencies to collect and monitor VMware data in the Splunk App for Infrastructure (SAI). You need to install components in the indexer tier. You don't install any components in the search head tier. After you install everything, you have to deploy a Data Collection Node (DCN) and Data Collection Scheduler (DCS) to collect VMware data.

VMware data collection requires a Splunk IT Service Intelligence (ITSI) license. To get all the components to collect VMware data, you have to download the ITSI package from Splunkbase.

To follow these steps, you have to have already configured SAI. If you haven't set up SAI yet, do that first. For information, see one of these topics:

- Install the Splunk App for Infrastructure in a single-instance deployment
- Install the Splunk App for Infrastructure in a distributed deployment

When you're done installing and configuring all the VMware data collection components, deploy a Data Collection Node (DCN) and Data Collection Scheduler (DCS) to configure data collection. For more information, see these topics:

- Deploy a Data Collection Node
- Deploy a Data Collection Scheduler

After you deploy a DCN and DCS, use a DCS to schedule data collection jobs for a DCN. For steps about how to collect VMware data, see these topics:

- Collect VMware vCenter Server metrics with Splunk App for Infrastructure
- Collect VMware vCenter Server and ESXi host log data with Splunk App for Infrastructure

Steps

Before you start, see VMware data collection planning and requirements. Follow these steps to install components for VMware data collection in a standalone or distributed Splunk Enterprise deployment.

1. Download Splunk IT Service Intelligence version

The VMware data collection components come with Splunk IT Service Intelligence (ITSI) from Splunkbase in the vmware_ta_itsi parent directory. These steps don't show you how to install ITSI. You just need to download the ITSI package for the required VMware data collection components you have to install. If you’re installing ITSI as well, see the Install and Upgrade Splunk IT Service Intelligence guide.

2. Install SA-VMWIndex, Splunk_TA_esxilog, and Splunk_TA_vcenter on indexers

Open the vmware_ta_itsi parent directory in the ITSI package and Install SA-VMWIndex, Splunk_TA_esxilog, and Splunk_TA_vcenter from the directory on every indexer that runs the Splunk Add-on for Infrastructure.

If you’re installing VMware data collection components in a non-clustered indexer environment, follow these steps.

1. On each indexer, copy the SA-VMWIndex, Splunk_TA_esxilog, and Splunk_TA_vcenter directories from the vmware_ta_itsi parent directory to the $SPLUNK_HOME/etc/apps directory.
2. Restart Splunk:
If you're installing VMware data collection components in a clustered indexer environment, follow these steps. For more information about this task, see Update common peer configurations and apps in the Managing Indexers and Clusters of Indexers guide.

1. On the machine that runs the indexer cluster master node, copy the SA-VMWIndex, Splunk_TA_esxilogs, and Splunk_TA_vcenter directories from the vmware_ta_itsi parent directory to the $SPLUNK_HOME/etc/master-apps directory.
2. Validate the bundle and check whether a restart is necessary:
   splunk validate cluster-bundle --check-restart
3. Apply the bundle to the indexer cluster:
   splunk apply cluster-bundle
4. To see how the cluster bundle push is going, run this command:
   splunk show cluster-bundle-status

Deploy a Data Collection Node

Deploy a Data Collection Node (DCN) to collect data from VMware vSphere vCenter Servers. You can deploy a DCN with the Splunk VMware OVA for ITSI or manually convert a heavy forwarder into a DCN.

After you deploy a DCN, configure data collection with a Data Collection Scheduler (DCS) from the Add Data page in the Splunk App for Infrastructure. For information about setting up a DCS, see Deploy a Data Collection Scheduler.

If you're collecting VMware vCenter Server data and migrate Python versions, you have to update your Data Collection Node configuration. For more information, see Update a Data Collection Node after migrating Python versions.

Prerequisites

- You viewed the DCN requirements. See Data Collection Node requirements and limits.

Deploy a DCN with the Splunk VMware OVA for ITSI

Deploy the Splunk VMware OVA for ITSI in a vCenter Server. When you deploy the OVA, it creates a virtual machine running a Splunk heavy forwarder that's configured to be a DCN. For information about specifications for the OVA, see Install and configure the OVA in the Install and Configure the Splunk VMware OVA for ITSI guide.

Follow these steps to deploy the OVA and set up the DCN.

1. **Download the Splunk VMware OVA for ITSI**

   Download the Splunk VMware OVA for ITSI from Splunkbase.

2. **Install the Splunk Add-on for Infrastructure inside the OVA**

   Install the Splunk Add-on for Infrastructure from Splunkbase inside the OVA for index time extractions.
3. Deploy the DCN in a vCenter Server

Use the OVA to create a virtual machine in your vCenter Server to run the DCN. For information about deploying an OVA, see Deploy an OVF or OVA Template on the VMware website.

For information about DCN requirements, see Data Collection Node requirements and limits.

After you deploy the OVA, the vCenter Server automatically assigns an IP address to the DCN via DHCP. For the most reliable connection, configure a static IP address for the DCN if possible.

Follow these steps to set up the DCN after you deployed the OVA in a vCenter Server.

1. SSH into the virtual machine that's running the DCN.
2. Log in to the virtual machine as the root user:
   
   username: root
   password: changemenow

3. Change the password:

   # passwd

4. Run the `dcn-network-config` command to test the network configuration for the DCN. Press Enter for each setting you don't want to change. When you finish, the `dcn-network-config` command tests your network configuration. These are the settings you can modify:

   - IPv4 address
   - IPv4 address of the default gateway
   - Netmask
   - DNS/Nameserver
   - Hostname

4. Configure the DCN

1. Log in to the virtual machine with these user credentials:

   username: splunk
   password: changeme

2. Run the `dcn-splunk-config` command and enter a new password for the admin user for the universal forwarder. Before you change the password for the admin user, the default password is changeme.

3. Configure these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter comma separated Indexers(&lt;host&gt;:&lt;port&gt;)[[]]</td>
<td>Enter the IP address and port of each indexer you want to forward data to. For more information about forwarding data directly to indexers, see Connect forwarders directly to peer nodes in the Splunk Enterprise Managing Indexers and Clusters of Indexers guide.</td>
</tr>
<tr>
<td>Enter license master(https://&lt;host&gt;:&lt;port&gt;)[self]</td>
<td>You don't have to configure the DCN as a license slave to collect data from the VMware vCenter Server. Press Enter to continue without providing a license master.</td>
</tr>
</tbody>
</table>

4. Save your changes and restart Splunk.

Configure a heavy forwarder to be a DCN

Follow these steps to configure an existing heavy forwarder as a DCN. If you use a heavy forwarder that's performing other tasks, you may run into performance issues. For the best performance, configure a heavy forwarder to be a
dedicated DCN, especially if you want to monitor vCenter Servers that are near or at the maximum number of ESXi hosts and virtual machines a DCN can manage. For information about DCN requirements and limits, see Data Collection Node requirements and limits.

Make sure that you're running a compatible version of Splunk Enterprise for the instance you configure as a DCN. For version requirements, see Version compatibility.

1. **Install the add-ons**

Install the following add-ons on the heavy forwarder. Download the Splunk ITSI package on Splunkbase and extract the add-ons. To install the add-ons, copy the directories from the `vmware_ta_itsi` parent directory in the ITSI package to `$SPLUNK_HOME/etc/apps`.

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk_TA_vmware</td>
<td>Runs a Python-based API data collection engine and performs search-time tagging of VMware data.</td>
</tr>
<tr>
<td>SA-Hydra</td>
<td>Runs worker processes to collect VMware data from vCenter Servers.</td>
</tr>
<tr>
<td>Splunk_TA_esxilogs</td>
<td>Runs props and transforms for ESXi log data you forward to the DCN. If you don't forward ESXi log data to the DCN and instead forward ESXi log data directly to the indexer tier, you don't have to install this add-on on the DCN.</td>
</tr>
<tr>
<td>Splunk_TA_vcenter</td>
<td>Runs props and transforms for vCenter Server log data you forward to the DCN. If you don't forward vCenter Server log data to the DCN and instead forward vCenter Server log data directly to the indexer tier, you don't have to install this add-on on the DCN.</td>
</tr>
</tbody>
</table>

Install the following add-on on the heavy forwarder. Download the Splunk Add-on for Infrastructure package on Splunkbase and install it under `$SPLUNK_HOME/etc/apps`.

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk_TA_Infrastructure</td>
<td>Contains all the index time extractions for VMware.</td>
</tr>
</tbody>
</table>

2. **Configure forwarding**

Configure the heavy forwarder to send data to your indexer or distributed indexer environment.

Follow these steps to configure forwarding:

1. Enable forwarding on the heavy forwarder. For information about deploying a heavy forwarder, see Set up forwarding in the Splunk Enterprise Forwarding Data guide.
2. Specify the indexer or group of indexers you want to forward data to. There are two options to do this:
   1. Manually specify each indexer you want to forward data to. For more information about forwarding data directly to indexers, see Connect forwarders directly to peer nodes in the Splunk Enterprise Managing Indexers and Clusters of Indexers guide.
   2. Configure indexer discovery to forward data to indexers. For information about how to use indexer discovery, see Use indexer discovery to connect forwarders to peer nodes.

**Configure additional settings for a DCN**

After you deploy the DCN, you can configure settings to change the limit for the count of metrics the DCN collects from a VMware vCenter Server, change the NTP server pool list, and disable NTP on the data collection node.
**Change the limit for the count of metrics the DCN collects**

As of VMware vCenter Server version 5.5 Update 2d, there's a 64 limit count of performance metrics that the `vpxd.stats.maxQueryMetrics` function collects. The vCenter Server calculates the count of performance metrics by multiplying the number of metrics by the number of virtual machines that you're querying. For example, if you query 10 metrics from eight virtual machines, that's a query size of 80.

If you hit the limit, you'll see a message like this:

`Request processing is restricted by administrator.`

For instructions on how to change the limit, see Performance charts are empty and displays the error: Request processing is restricted by administrator (2107096) on the VMware Knowledge Base website.

**Change the NTP server pool list**

A system uses the Network Time Protocol (NTP) to synchronize its time with another reference time source. If you're experiencing time synchronization issues between the indexer, DCN, and vCenter Server, change the NTP servers that the DCN uses.

1. On the instance running the DCN, go to `/etc/ntp.conf`. These are the following values:

   ```
   # Use public servers from the pool.ntp.org project.
   # Please consider joining the pool (http://www.pool.ntp.org/join.html).
   server 0.centos.pool.ntp.org
   server 1.centos.pool.ntp.org
   server 2.centos.pool.ntp.org
   ```

2. Replace the default values in the file with your NTP server values.
3. Restart `ntpd`:

   ```
   $ sudo service ntpd restart
   ```

**Disable NTP on the DCN**

If you deployed a DCN in a vCenter Server and it doesn't have internet access, disable NTP on the DCN. If you disable NTP, enable VMware Tools Clock Synchronization to establish the time for the DCN using the ESXi host.

1. Stop `ntpd`:

   ```
   $ sudo service ntpd stop
   ```

2. Configure `ntpd` so that it doesn't run when the system starts:

   ```
   $ sudo chkconfig ntpd off
   ```

3. Enable VMware Tools Clock Synchronization:

   ```
   $ vmware-toolbox-cmd timesync enable
   ```

4. Confirm that VMware Tools Clock Synchronization is enabled:

   ```
   $ vmware-toolbox-cmd timesync status
   ```

**Deploy a Data Collection Scheduler**

---

34
Deploy a Data Collection Scheduler (DCS) to integrate VMware vSphere vCenter Servers and manage each Data Collection Node (DCN) you deploy. A DCS schedules jobs and manages DCNs that collect data from vCenter Servers. There are a few places to deploy the DCS:

- You can modify a Data Collection Node (DCN) to also act as a DCS.
- If you’re running a single-instance search head environment, you can deploy the DCS on the search head.
- If you’re running a distributed search head environment, you can deploy the DCS on a dedicated Splunk Enterprise instance or modify a DCN to also act as a DCS.

When you integrate a VMware vCenter Server on a DCS, you have to provide credentials for a user account associated with the vCenter Server on the DCS. For information about user account requirements, including the permissions the user account needs to have, see User account permissions.

Prerequisites

- You viewed the DCS requirements. See Data Collection Scheduler requirements.
- You have an available Splunk Enterprise instance running CentOS 6 or 7. For more information, see Install on Linux in the Splunk Enterprise Installation Manual.

Steps

Follow these steps to deploy a DCS.

1. **Install the app and add-ons**

Download the Splunk App for Infrastructure (SAI) version 2.0.0 on Splunkbase.

Download the Splunk IT Service Intelligence (ITSI) version 4.4 package on Splunkbase and extract these add-ons:

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk_TA_vmware</td>
<td>Runs a Python-based API data collection engine and performs search-time tagging of VMware data.</td>
</tr>
<tr>
<td>SA-Hydra</td>
<td>Runs worker processes to collect VMware data from vCenter Servers.</td>
</tr>
</tbody>
</table>

To install SAI, put the `splunk-app-for-infrastructure_200` directory in the `$SPLUNK_HOME/etc/apps` directory on the Splunk Enterprise instance.

To install the add-ons from the ITSI package, copy `Splunk_TA_vmware` and `SA-Hydra` from the ITSI version 4.4 package to the `$SPLUNK_HOME/etc/apps` directory on the Splunk Enterprise instance.

2. **Configure your ITSI license**

Add your ITSI license to the Splunk Enterprise instance. You have two options to add your license to the instance:

- Install the license manually. For more information, see Install a license in the Splunk Enterprise Admin Manual.
- Configure the instance as a license slave. For more information, see Configure a license slave in the Splunk Enterprise Admin Manual.

3. **Start integrating VMware vCenter Servers and manage DCNs**

Integrate Data Collection Nodes (DCNs) and vCenter Servers on a DCS. If you have multiple DCSs, you have to integrate a DCN and vCenter with the same DCS. For example, if you deployed 3 DCSs to manage VMware data collection, and
you configured DCN A to collect data from vCenter B, use DCS 1 to manage DCN A and integrate vCenter B.

If you haven't deployed a DCN yet, do that now. For more information, see Deploy a Data Collection Node.

To integrate a vCenter, see Collect VMware vCenter Server metrics with Splunk App for Infrastructure.

**Change default collection intervals**

After you deploy the DCN, you can modify default collection intervals. Change collection intervals to reduce the load on your Data Collection Nodes (DCNs) and your vCenter Servers. First change the time interval for host inventory jobs, then change the time interval for host performance data. The unit of time for collection intervals is seconds.

1. On the instance that runs the DCS, go to `$SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local`
2. Open the `pool.conf` file. If the file doesn't exist yet, create it now.
3. In the `[Global pool]` stanza, change the `hostinv_interval` and `hostinv_expiration` values. If the `[Global pool]` stanza doesn't exist, create it.
4. Change values for `hostinv_interval` and `hostinv_expiration`. These settings have to have the same values. The maximum value is 2700.
5. Change values for `hostvmperf_interval` and `hostvmperf_expiration`. These settings have to have the same values. The maximum value is 1200.
6. Save your changes and exit.
Upgrade VMware data collection components

Upgrade VMware data collection components

To collect VMware data in SAI, you have to install components in the Splunk VMware Add-on for ITSI from the Splunk IT Service Intelligence (ITSI) package. You can't use earlier versions of the Splunk Add-on for VMware.

The Splunk VMware Add-on for ITSI sends metrics to the `vmware-perf-metrics` metrics index. Previous versions of the Splunk Add-on for VMware send data to the `vmware-perf events` index. If you want to search historical event data in the `vmware-perf events` index, include the `vmware-perf` index in `indexes.conf`. For more information, see Search historical data after you upgrade.

These steps show you how to upgrade the VMware data collection components from an earlier version of `vmware_ta_itsi` and the Splunk Add-on for VMware version 3.4.x.

Stop the DCS before upgrading the DCS, DCN, and each indexer. After you upgrade everything, start the DCS.

Upgrade a Data Collection Scheduler

Replace the required components and delete old components that aren't necessary for VMware data collection in SAI on the Data Collection Scheduler (DCS).

**Upgrade a DCS running an earlier version of vmware_ta_itsi**

Follow these steps to upgrade a DCS that's running an earlier version of `vmware_ta_itsi`.

1. If you haven't already, download the ITSI package from Splunkbase.
2. In the ITSI user interface, click the Add Data tab and select VMware vSphere.
3. Select the DCN tab and disable Enable Data Collection.
4. Stop splunkd.

   ```bash
   $SPLUNK_HOME/bin/splunk stop
   ```

5. Copy the SA-Hydra and Splunk_TA_vmware directories from the `vmware_ta_itsi` parent directory in the ITSI package to `$SPLUNK_HOME/etc/apps`.

   ```bash
   $SPLUNK_HOME/bin/splunk start
   ```

**Upgrade a DCS running the Splunk Add-on for VMware version 3.4.x**

Follow these steps to manually upgrade a DCS that's running the Splunk Add-on for VMware version 3.4.x.

1. If you haven't already, download the ITSI package from Splunkbase.
2. Stop the DCS from the Collection Configuration page in the Splunk Add-on for VMware version 3.4.x.
3. Stop splunkd.

   ```bash
   $SPLUNK_HOME/bin/splunk stop
   ```

4. Copy the SA-Hydra and Splunk_TA_vmware directories from the `vmware_ta_itsi` parent directory in the ITSI package to `$SPLUNK_HOME/etc/apps`.
5. If any of these directories exist in `$SPLUNK_HOME/etc/apps`, remove them.
6. In $SPLUNK_HOME/etc/apps/SA-Hydra, remove the appserver directory.
7. In $SPLUNK_HOME/etc/apps/SA-Hydra/bin/hydra, remove the uuid.py and uuid.pyc files.
8. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware, remove the appserver directory.
9. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin, remove the suds directory, and the uuid.py and uuid.pyc files.
10. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/default, remove the data directory.
11. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local, remove inputs.conf.
12. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local, create pool.conf if it doesn’t exist already.

1. Open pool.conf.
3. Move only task-related parameters from the [default] stanza in ta_vmware_collection.conf to the [Global pool] stanza you just created. This include task, atomic_tasks, <task>_expiration, and <task>_interval.
4. Replace otherperf with clusterperf. For example, rename otherperf_interval to clusterperf_interval.
5. Remove hierarchyinv and rpinv parameters from the task and atomic_tasks settings if they exist.
6. Remove interval and expiration parameters for hierarchyinv and rpinv if they exist.
7. Keep collection parameters other than task-related in ta_vmware_collection.conf.
8. If your ta_vmware_collection.conf file looks like this:

```
[default]
job = vminv, hostinv, otherperf, rpinv, hierarchyinv
vminv_interval = 900
vminv_expiration = 900
hostinv_interval = 900
hostinv_expiration = 900
otherperf_interval = 1800
otherperf_expiration = 1800
hierarchyinv_interval = 1800
hierarchyinv_expiration = 1800
rpinv_interval = 1800
rpinv_expiration = 1800
deployment_type = Custom
perf_format_type = normal
host_instance_whitelist = \.*ahegd.*
```

Move these parameters to pool.conf:

```
[Global pool]
job = vminv, hostinv, clusterperf
vminv_interval = 900
vminv_expiration = 900
hostinv_interval = 900
hostinv_expiration = 900
clusterperf_interval = 1800
clusterperf_expiration = 1800
```

These are the remaining parameters in ta_vmware_collection.conf:

```
[default]
deployment_type = Custom
perf_format_type = normal
host_instance_whitelist = \.*ahegd.*
```
13. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local, make these changes:
   1. Open hyrda_node.conf and add pool_name = Global pool to every stanza.
   2. Open ta_vmware_collection.conf and add pool_name = Global pool to every stanza except the default stanza.

   $SPLUNK_HOME/bin/splunk start

**Upgrade a Data Collection Node**

Replace the required components and delete old components that aren't necessary for VMware data collection in SAI on the Data Collection Node (DCN).

**Upgrade a DCN running an earlier version of vmware_ta_itsi**

Follow these steps to upgrade a DCN that's running an earlier version of vmware_ta_itsi.

1. If you haven't already, download the ITSI package from Splunkbase.
2. Stop splunkd.

   $SPLUNK_HOME/bin/splunk stop

3. Copy the SA-Hydra, Splunk_TA_vmware, Splunk_TA_esxilogs, and Splunk_TA_vcenter directories from the vmware_ta_itsi parent directory in the ITSI package to $SPLUNK_HOME/etc/apps.
4. Start splunkd.

   $SPLUNK_HOME/bin/splunk start

**Upgrade a DCN running the Splunk Add-on for VMware version 3.4.x**

Follow these steps to manually upgrade a DCN that's running the Splunk Add-on for VMware version 3.4.x.

1. If you haven't already, download the ITSI package from Splunkbase.
2. Stop splunkd.

   $SPLUNK_HOME/bin/splunk stop

3. Copy the SA-Hydra, Splunk_TA_vmware, Splunk_TA_esxilogs, and Splunk_TA_vcenter directories from the vmware_ta_itsi parent directory in the ITSI package to $SPLUNK_HOME/etc/apps.
4. If any of these directories exist in $SPLUNK_HOME/etc/apps, remove them:
   - SA-VMNetAppUtils
   - SA-VMWIndex
   - TA-VMW-FieldExtractions
5. In $SPLUNK_HOME/etc/apps/SA-Hydra, remove these directories:
   - local
   - appserver
6. In $SPLUNK_HOME/etc/apps/SA-Hydra/bin/hydra, remove the uuid.py and uuid.pyc files.
7. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware, remove the appserver directory.
8. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/bin, remove the suds directory, and the uuid.py and uuid.pyc files.
9. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local, remove these files:
   - inputs.conf
   - ta_vmware_cache.conf
   - hydra_metadata.conf
   - hydra_session.conf
10. In $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/default, remove the data directory.
11. Start splunkd.
$SPLUNK_HOME/bin/splunk start

Upgrade an indexer

Replace the required components and delete old components that aren't necessary for VMware data collection in SAI on each indexer. You can follow these steps if you're running a standalone indexer, a distributed indexer, or a clustered indexer environment.

If you want to continue searching data you already collected from the Splunk Add-on for VMware version 3.4.x, add the old index to the new indexes.conf in SA-VMWIndex during the upgrade process. If you don't include the old index before you start splunkd after upgrading, the indexer deletes the index. For more information, see Search historical data after you upgrade.

For more information about installing the add-on across an indexer cluster, see Update common peer configurations and apps in the Managing Indexers and Clusters of Indexers guide.

**Upgrade an indexer running an earlier version of vmware_ta_itsi**

Follow these steps to upgrade an indexer that's running an earlier version of vmware_ta_itsi.

1. If you haven't already, download the ITSI package from Splunkbase.
2. Stop splunkd:
   
   $SPLUNK_HOME/bin/splunk stop
3. Copy the SA-VMWIndex, Splunk_TA_esxilogs, and Splunk_TA_vcenter directories from the vmware_ta_itsi parent directory in the ITSI package to $SPLUNK_HOME/etc/apps. If you want to continue monitoring historical data, add the old index to the new indexes.conf in SA-VMWIndex. If you don't include the old index, the indexer deletes the index. See Search historical data after you upgrade.
4. Start splunkd:
   
   $SPLUNK_HOME/bin/splunk start

**Upgrade an indexer running the Splunk Add-on for VMware version 3.4.x**

Following these steps to update an indexer that's running the Splunk Add-on for VMware version 3.4.x.

1. If you haven't already, download the ITSI package from Splunkbase.
2. Stop splunkd:
   
   $SPLUNK_HOME/bin/splunk stop
3. Copy the SA-VMWIndex, Splunk_TA_esxilogs, and Splunk_TA_vcenter directories from the vmware_ta_itsi parent directory in the ITSI package to $SPLUNK_HOME/etc/apps. If you want to continue monitoring historical data, add the old index to the new indexes.conf in SA-VMWIndex. If you don't include the old index, the indexer deletes the index. See Search historical data after you upgrade.
4. If any of these directories exist in $SPLUNK_HOME/etc/apps, remove them.
   - SA-VMNetAppUtils
   - SA-VMWIndex
   - TA-VMW-FieldExtractions
5. Start splunkd:
   
   $SPLUNK_HOME/bin/splunk start
Search historical data after you upgrade

You can continue searching historical data that the Splunk Add-on for VMware version 3.4.5 indexed. To do so, you have to add the `vmware-perf` stanza to `$SPLUNK_HOME/etc/apps/SA-VMWIndex/local`.

Follow these steps to search historical data after you upgrade to the Splunk VMware Add-on for ITSI.

1. Stop splunkd:
   ```
   $SPLUNK_HOME/bin/splunk stop
   ```

2. In `$SPLUNK_HOME/etc/apps/SA-VMWIndex/local`, create `indexes.conf` if it doesn't already exist.

3. Open `indexes.conf` and add this stanza:
   ```
   [vmware-perf]
   homePath = $SPLUNK_DB/vmware-perf/db
   coldPath = $SPLUNK_DB/vmware-perf/colddb
   thawedPath = $SPLUNK_DB/vmware-perf/thaweddb
   repFactor = auto
   ```

4. Start splunkd:
   ```
   $SPLUNK_HOME/bin/splunk start
   ```

Update a Data Collection Node after migrating Python versions

When you migrate Splunk Enterprise to a different version of Python, Data Collection Nodes (DCN) stop receiving jobs for worker processes that collect data from a VMware vCenter Server. To continue collecting vCenter Server data with a DCN, you have to clear the cache, metadata, and session information on the DCN. To do this, remove the local `ta_vmware_cache.conf`, `hydra_session.conf`, and `hydra_metadata.conf` files in $SPLUNK_TA_vmware.

Until you remove the required files, you'll see this error in worker process logs:

```
Error: UnicodeDecodeError: 'ascii' codec can't decode byte 0xe3 in position 1: ordinal not in range(128) in Scheduler and Worker logs
```

The log files for worker processes look like these:

**Hydra worker logs**

```
```
return self.set_entity_fields(entity)

File "opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
    from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
File "opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
    obj = cPickle.loads(b64decode(val))
UnicodeDecodeError: 'ascii' codec can't decode byte 0xe3 in position 1: ordinal not in range(128)

Hydra scheduler logs

2019-10-10 00:28:39,115 ERROR [ta_vmware_collection_scheduler://Global pool] [HydraWorkerNode]
node=https://<worker-ip>:8089 is dead, because some weird stuff happened: 'ascii' codec can't decode byte
0xe3 in position 1: ordinal not in range(128)
Traceback (most recent call last):
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 1462, in setMetadata
    self.session_key)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 610, in from_name
    host_path=host_path)
  File "/opt/splunk/lib/python3.7/site-packages/splunk/models/base.py", line 557, in get
    return self._from_entity(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 345, in _from_entity
    obj.from_entity(entity)
  File "/opt/splunk/lib/python3.7/site-packages/splunk/models/base.py", line 926, in from_entity
    super(SplunkAppObjModel, self).from_entity(entity)
  File "/opt/splunk/lib/python3.7/site-packages/splunk/models/base.py", line 684, in from_entity
    return self.set_entity_fields(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
    from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
    obj = cPickle.loads(b64decode(val))
UnicodeDecodeError: 'ascii' codec can't decode byte 0xe3 in position 1: ordinal not in range(128)

Steps

Follow these steps to clear the cache, metadata, and session information on a DCN so the DCN continues collecting
VMware vCenter Server data after you migrate to a new Python version.

1. Stop the DCS that you used to integrate the DCN.
2. Stop splunkd on the DCN:
   $SPLUNK_HOME/bin/splunk stop
3. On the DCN, go to $SPLUNK_HOME/etc/apps/Splunk_TA_vmware/local and delete these files:
   • ta_vmware_cache.conf
   • hydra_session.conf
   • hydra_metadata.conf
4. Start splunkd on the DCN:
   $SPLUNK_HOME/bin/splunk start
5. Start the DCS that you used to integrate the DCN.
   1. Open Splunk Web for the Splunk Enterprise instance that runs the DCS.
   2. Go to the Splunk App for Infrastructure.
   3. Go to the Add Data tab and select VMware vSphere in the integrations panel.
   4. Select the DCN tab and enable data collection.