VMware Skyline Collector User Guide

VMware Skyline 1.4

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Skyline Collector User Guide

1

The VMware Skyline Collector User's Guide provides instructions for working with the VMware® Skyline™ Collector. The document contains information about registering for VMware Skyline services, configuring data collection, and a section about the privacy and security of the information VMware receives.

Intended Audience

This information is intended for anyone who wants to work with the VMware Skyline Collector. It is written for VMware® vSphere® administrators.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to https://www.vmware.com/support/pubs/

Log In to Skyline Collector

2

This section describes how to log into the Skyline Collector.

Log into the Skyline Collector to review the status and make configuration changes to the Skyline Collector.

Prerequisites

- Obtain the IP address or fully qualified domain name of the Skyline Collector within the vSphere Web Client.

Procedure

1. Open a web browser and enter the URL for the Skyline Collector.
   `https://skyline_collector_ip_address_or_fqdn`
2. Enter the user name **`admin`** and associated **`password`**.
3. Click **Log In**.

Skyline Collector User Interface

3

This section provides an overview of the Skyline Collector User Interface.

The Skyline Collector User Interface contains two primary sections, System Status and Configuration.

System Status

4

This topic provides a description of the System Status page.

The left side of the **System Status** page provides you with an overview of the VMware Skyline Collector health, management capabilities. The system status includes Stop, Start, and Restart and each endpoint connected to the VMware Skyline Collector for the data collection.

The Overview section of the **System Status** page displays the overall health of the Skyline Collector, which typically is in a 'Your collector is running' state. Also, the health of each configured data endpoint is displayed.

The **Collector** section allows you to manage the Skyline Collector. From here, you can Restart, Stop, or Deregister the Skyline Collector service. The Skyline Collector ID and My VMware user which was used to register the Skyline Collector is displayed. The Skyline Collector ID is a unique identifier for your specific Skyline Collector instance. It is used to identify the information sent back to VMware. You can also use the Skyline Collector friendly name to identify your Skyline Collector instance when working with VMware Global Support Services (GSS). The Entitlement number and support type (Production Support or Premier Services) are also displayed. The entitlement accounts link the Skyline Collector data to support requests. Entitlement accounts are managed through https://my.vmware.com.

If needed, the most recent Skyline Collector log activity can be displayed within the user interface.

Endpoints

For each vCenter Server that the Skyline Collector is connected to, there are three endpoints configured. Also, the endpoint health is displayed.

- VC_CHANGES

  The VC_CHANGES endpoint type collects vCenter topology and configuration information.

- VC_EVENTS

  The VC_EVENTS endpoint type collects vCenter event information.

- VC_HOSTS

  The VC_HOSTS endpoint type collects ESXi event information (through vCenter Server).

For each NSX Manager that the Skyline Collector is connected to, there are three endpoints configured. Also, the endpoint health is displayed.

- NSX

  The NSX endpoint type collects NSX product and configuration information.

- NSX_TELEMETRY

  The NSX_TELEMETRY endpoint type collects NSX operational metrics information, such as CPU, memory, and disk use.

- NSX_EVENTS

  The NSX_EVENTS endpoint type collects NSX event information.

Each endpoint displays the name of the product instance that it is connected to, the account currently used to capture data and the last time data collected by that endpoint collection instance. Endpoints that are started and actively collecting data is shown in green, while endpoints that are stopped or have issues are shown in red.

Configuration

5

This topic provides a brief description of the Configuration page.

The following actions can be performed within the **Configuration** page of the Skyline Collector User Interface.

- Adding a vCenter Server for the data collection.
- Deleting a vCenter Server from the data collection.
- Adding an NSX Manager for the data collection.
- Delete an NSX Manager from the data collection.
- Configuring Auto-Upgrade.
- Defining a Friendly Name.
- Configuring Active Directory authentication.

This chapter includes the following topics:

Add a vCenter Server

This section describes how to add a vCenter Server to the Skyline Collector.

Prerequisites

- A user account with the following vCenter Server permissions is required to configure vCenter Server for the product use data collection.
  - vCenter Server read-only role
  - Global > License

Procedure

1. Click **Configuration** within the Skyline Collector User Interface.
2. Click **vCenters**.
3. Click **Add vCenter**.
4. Product instances configured for the product use data collection participate within the Customer Experience Improvement Program (CEIP). For information, visit: https://www.vmware.com/solutions/trustvmware/ceip.html. Click **Continue**.
5. Enter the vCenter Server details.
   a. Enter the vCenter Server **`IP address`** or **`fully-qualified domain name (FQDN)`**.
   b. Enter the vCenter Server read-only user account **`Username`**.
   c. Enter the **`Password`** for the user account specified in the previous step.
6. If you are using an external Platform Services Controller (PSC), Single-Sign On (SSO) provider or have a custom SSO domain, toggle the Use Custom SSO Configuration switch to **Yes**.
   a. Enter the PSC/SSO server **`IP address`** or **`fully-qualified domain name (FQDN)`**.
   b. If you are using the default PSC/SSO provider configuration, you DO NOT have to complete the Advanced Options (optional) text boxes. You only have to complete the **SSO Admin URL**, **SSO STS URL** , and **Lookup Service URL** if you specified a custom configuration during the deployment of your PSC or SSO provider.
   c. If you do not want to collect product use data from all data centers connected to the vCenter Server you are configuring, toggle the Collect from all data centers switch to **No**, then click **Add**. An invalid certificate warning might appear. The certificate is expected, click **Continue**. Select the **checkbox** next to each data center that you want to collect product use data for. When finished selecting data centers, click **Enable Selected Datacenters**.
7. To add this vCenter Server to the Skyline Collector, click **Add** . You now begin receiving proactive findings and recommendations for all objects (data centers) managed by this vCenter Server.

Note Disabling product use data collection from data centers might prohibit VMware from providing an optimal support experience.

Add an NSX Manager

This section describes how to add an NSX Manager to the Skyline Collector.

Prerequisites

- A user account with the following NSX Manager permissions is required to configure NSX Manager for the product use data collection.
  - NSX Manager built-in Auditor role.

Procedure

1. Click **Configuration** with the Skyline Collector User Interface.
2. Click **NSX Managers**.
3. Click **Add NSX Manager**.
4. Product instances configured for the product use the data collection participates within the Customer Experience Improvement Program (CEIP). For information, visit: https://www.vmware.com/solutions/trustvmware/ceip.html. Click **Continue**.
5. Enter the NSX Manager details.
   a. Enter the NSX Manager **`IP address`** or **`fully-qualified domain name (FQDN)`**.
   b. Enter the NSX Manager user account **`Username`**.
   c. Enter the **`Password`** for the user account specified in the previous step.
6. To add this NSX Manager to the Skyline Collector, click **Add**. You now begin receiving proactive findings and recommendations for the NSX environment manged by this NSX Manager.

Configure a Proxy

This section describes how to configure a Proxy for the Skyline Collector.

The Skyline Collector uploads encrypted product use data to VMware using the Internet. If required by your organization, an HTTP proxy server can be configured between the Skyline Collector and the Internet.

Procedure

1. Click **Configuration**.
2. Click **Proxy**.
3. Click **Add Proxy**.
4. Enter the Proxy Server **`IP Address`**.
5. Enter the Proxy Server **`Port`**.
6. If needed, enter the Proxy Server **`username`**.
7. If needed, enter the Proxy Server **`password`** for the user name specified in the previous step.
8. Click **Add Proxy Configuration**.

Auto-Upgrade

This section describes how to enable the auto-upgrade for the Skyline Collector.

If an update is available, the Skyline Collector supports the ability to upgrade automatically. Auto-Upgrade checks for and install updates to the Skyline Collector at a specific time and day of the week that you specify.

Prerequisites

- The Skyline Collector must be able to receive update notifications from vapp-updates.vmware.com. For more details regarding networking requirements, see the Skyline Collector Installation and Configuration Guide.

Procedure

1. Click **Configuration**.
2. Click **Auto-Upgrade**.
3. Select your auto-upgrade configuration.
   a. From the **dropdown menu**, select a day of the week for the Skyline Collector to select for and install updates, if available.
   b. From the **dropdown menu**, select a time of the day for the Skyline Collector to select for and install updates, if available.
4. To save your settings, click **Set Upgrade Configuration**.

After each collector auto-upgrade, an email notification will be sent to the My VMware email address used during the initial configuration.

Collector Name

This section describes how to create a friendly name for the Skyline Collector.

A friendly name is intended to describe the environment you are configuring the Skyline Collector to collect data from. This name is used to make it easier for VMware GSS to communicate information about the Skyline Collector with you.Example: East-Production

Procedure

1. Click **Configuration**.
2. Click **Collector Name**.
3. Enter a **`Collector Friendly Name`**.
4. Click **Set Friendly Name**.

Active Directory

This section describes how to configure Active Directory authentication to the Skyline Collector user interface.

Active Directory (AD) can be enabled to allow access for specific AD Users and Groups to the Skyline Collector user interface. Active Directory allows for more granular access controller to the user interface and restricts the number of individuals that might need to know the admin user account details.

To configure Active Directory (AD) authentication, follow these steps :

Prerequisites

- To enable Active Directory authentication, anonymous bind must be enabled within Active Directory. Do not enable anonymous bind only for the purpose of enabling Active Directory authentication to the Skyline Collector user interface.

Procedure

1. Click **Configuration**.
2. Click **Active Directory**.
3. Toggle the Do you want to enable Active Directory switch to **Yes**.
4. Enter the Domain Controller **`IP address`** or **`fully qualified domain name`**.
5. Enter the **`Port`**.
6. Enter the **`Domain Name`**.
7. Enter an Active Directory User or Group by typing in the space provided.

   Note

   - You do not need to provide domain details when adding a User or Group.
     - For example, if you wanted to add the user Support Admin (DOMAIN\supportadmin), enter supportadmin on the line provided within Allowed AD Users, and click **Add User**.
   - Active Directory (AD) Groups added to Skyline Collector are not recursive. Any AD Groups that reside within the AD Group (subgroup) that you are adding are not granted access to the user interface. Only AD Users of the specific AD Group you are adding have access to the Skyline Collector user interface.

8. Click **Set Active Directory Configuration**.

Note If an Active Directory User logs into the Skyline Collector user interface, there is no option to Manage AD from the Settings page. The ability to Manage Active Directory is only available to the admin account.

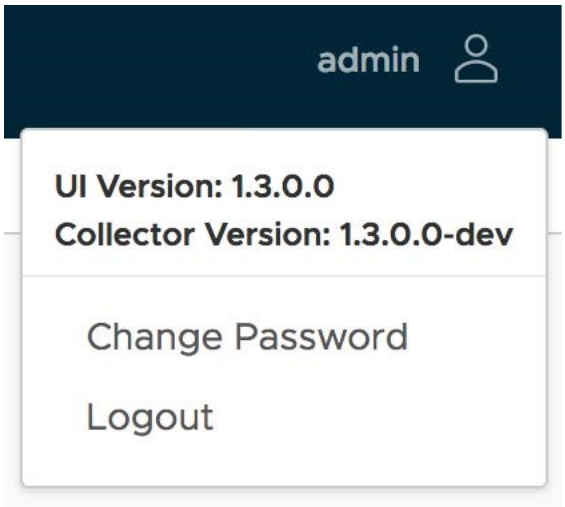
Changing the Admin Password

6

This section describes how to change the Skyline Collector admin user account password.

The Skyline Collector admin user account password can be changed at any time by selecting the admin account at the top-right of the Skyline Collector user interface. A **drop-down** menu appears. Select **Change Password**.

Figure 6-1. Admin User Menu



The new password must meet the password complexity policy as described on the Change Password page. After entering the old and new password for the admin account, Select **Set Password** to save the new password.

Manage Endpoints

7

This section describes how to manage the associated endpoints for each configured VMware product (vCenter Server and NSX Manager).

To manage endpoints currently configured for the Skyline Collector, click **System Status** .

For each endpoint, there are three actions that can be performed, **Restart**, **Stop**, and **Start**. The Start action is not available when the endpoint is running. The Start action becomes available when the endpoint is stopped.

Restart the endpoint collection stops and starts endpoint collection for that endpoint.

Stop endpoint collection temporarily pauses the collection of that endpoint.

Start endpoint collection starts the collection process for that endpoint. **Start** is available only when an endpoint is in a Stopped status.

you have the option to **Start** the endpoint collection process for that endpoint.

Details including the product endpoint (vCenter Server, NSX Manager), and the user account being used to connect the Skyline Collector to the product endpoint is displayed. The Data Centers for which the endpoint is collecting data from is also displayed.

The size of the payload uploaded to the VMware Analytics Cloud and the last upload occurred is displayed for each endpoint.

The latest logs can be viewed within each endpoint. You can view the latest logs when want to review system activity or during Skyline Collector troubleshooting.

Manage Collector

8

This section describes how to manage the Skyline Collector.

The **Collector** section within the **System Status** page provides the following capabilities and information:

- **Start**, **Stop**, **Restart** , and **Deregister** the Collector.
- Skyline Collector unique identifier (ID).
- My VMware account which was used to register the Skyline Collector with VMware.
- Customer Entitlement Account details and current Support type.

Restarting the Skyline Collector is not needed and is available to aid in troubleshooting. Restarting normally take between 3 and 5 minutes to complete. The Skyline Collector admin interface might not be responsive during this time.

Stopping the Skyline Collector prevents any data from being sent to VMware. Do not stop the Skyline Collector unless troubleshooting with VMware support. If the Skyline Collector is in a Stopped status, an alert appears within the user interface stating Your Collector is not running. Use the **Start** action to restart the Skyline Collector.

Note Stopping the Skyline Collector within the user interface does not shut down the virtual appliance. The virtual appliance remains running and the user interface remains responsive.

De-registration permanently removes the collector entirely from the Skyline platform. The process also removes all configuration information, disables all endpoint collection, and resets the collector state back to the default, in addition to removing participation for the Skyline Collector from the Customer Experience Improvement Program (CEIP). Enabling the Skyline Collector after de-registration requires a user to go through initial configuration again and might require refreshing the browser. To de-register, enter your MyVMware account credentials and click **De-register**.

Note De-registering the Skyline Collector removes participation in the Customer Experience Improvement Program (CEIP) for that individual Skyline Collector instance only. Other installations of the Skyline Collector appliance are not impacted or updated.

9 Updating the Skyline Collector

This section describes how to update the Skyline Collector.

If you select not to enable Auto-Upgrade, follow these steps to update the Skyline Collector to the latest version using the VMware Appliance Management Interface (VAMI).

Procedure

1. Open a web browser and enter the URL for the Skyline Collector VAMI: **`https://skyline_collector_ip_address_or_fqdn:5480`**
2. Enter the user name **`root`** and associated **`password`**.
3. Click **Login**.
4. Click **Update**.
5. Click **Check Updates**.
6. If a new update is available, click **Install Updates**.

Participating in the Customer Experience Improvement Program (CEIP)

10

This section describes participating in the Customer Experience Improvement Program (CEIP).

Participation in the VMware Customer Experience Improvement Program (CEIP) is required as part of VMware Skyline. Joining this program is done as part of the initial configuration of the Skyline Collector.

Adding endpoints to the Skyline Collector sends product data to VMware for that product instance as part of the Customer Experience Improvement Program (CEIP). End points are added as part of the initial configuration or later through the **Configuration** page.

Participation in the Customer Experience Improvement Program (CEIP) can be discontinued for a Skyline Collector at any time by de-registering the Skyline Collector described in Manage Collector.

Categories of Information that VMware Receives

11

This section describes the categories of information that VMware receives.

As part of the Enhanced Support - Customer Experience Improvement Program (CEIP), VMware regularly collects technical information about your organization's use of VMware products and services in association with your organization's VMware license keys . Depending on the nature of the VMware product or service, the technical information collected consists of:

- Configuration Data

  Data about how you have configured VMware products and services and information related to your IT environment. Examples of Configuration Data include: version information for VMware products, product environment information, product configuration settings, and technical data relating to the devices accessing those products and services.

- Feature Usage Data

  Data about how your organization uses VMware product features and services. Examples of Feature Usage Data include: details about which product features your organization uses and metrics of user interface activity without personally identifying the user.

- Performance Data

  Data about the performance of VMware products and services. Examples of Performance Data include metrics of the performance and scale of VMware products and services, response times for User Interfaces, and details about your API calls.

- Product Log Data

  Product Logs generated by VMware products during the active deployment of the product. Typically, logs record system events and state during product operations. These logs do not contain customer workload content.