Subscription Central 1-latest

Using Discovery

Understanding Discovery

Last Updated: 2024-03-07

Subscription Central 1-latest Using Discovery

Understanding Discovery

Legal Notice

Abstract

Table of Contents

CHAPTER 1. ABOUT DISCOVERY

Discovery is designed to help users collect data about their usage of specific Red Hat software. By using Discovery, users can reduce the amount of time and effort that is required to calculate and report usage of those Red Hat products.

Learn more

To learn more about the purpose, benefits, and characteristics of Discovery, see the following information:

- What is Discovery?

To learn more about the products and product versions that Discovery can find and inspect, see the following information:

- What products does Discovery find?

To evaluate whether Discovery is a correct solution for you, see the following information:

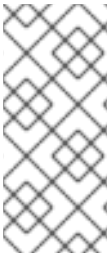
- Is Discovery right for me?

1.1. WHAT IS DISCOVERY?

Discovery is an inspection and reporting tool. It is designed to find, identify, and report environment data, or facts, such as the number of physical and virtual systems on a network, their operating systems, and other configuration data. In addition, it is designed to find, identify, and report more detailed facts for some versions of key Red Hat packages and products for the IT resources in that network.

The ability to inspect the software and systems that are running on your network improves your ability to understand and report on your subscription usage. Ultimately, this inspection and reporting process is part of the larger system administration task of managing your inventories.

Discovery requires the configuration of two basic structures to access IT resources and run the inspection process. A *credential* contains user access data, such as the username and password or SSH key of a user with sufficient authority to run the inspection process on a particular source or some of the assets on that source. A *source* contains data about a single asset or multiple assets that are to be inspected. These assets can be physical machines, virtual machines, or containers, identified as hostnames, IP addresses, IP ranges, or subnets. These assets can also be a systems management solution such as vCenter Server or Red Hat Satellite Server, or can be clusters deployed on Red Hat OpenShift Container Platform.



NOTE

Currently, the only virtualized deployment that discovery can scan with a specialized source for virtualization infrastructure is VMware vCenter. No other virtualization infrastructure that is supported by Red Hat can be scanned with a specialized scan. General scans of your network might still find these assets, without the precise metadata returned by a specialized scan.

You can save multiple credentials and sources to use with Discovery in various combinations as you run inspection processes, or *scans*. When you have completed a scan, you can access these facts in the output as a collection of formatted data, or *report*, to review the results.

By default, the credentials and sources that are created during the use of Discovery are encrypted in a

database. The values are encrypted with AES-256 encryption. They are decrypted when the Discovery server runs a scan with the use of a vault password to access the encrypted values that are stored in the database.

Discovery is an agentless inspection tool, so there is no need to install the tool on every source that is to be inspected. However, the system that Discovery is installed on must have access to the systems to be discovered and inspected.

1.2. WHAT PRODUCTS DOES DISCOVERY FIND?

Discovery finds the following Red Hat products. For each version or release, the earliest version is listed, with later releases indicated as applicable.

If a product has changed names recently so that you might be more familiar with the current name for that product, that name is provided as additional information. No later version is implied by the inclusion of a newer product name unless specific versions of that product are also listed.

Red Hat Enterprise Linux

- Red Hat Enterprise Linux version 5 and later
- Red Hat Enterprise Linux version 6 and later
- Red Hat Enterprise Linux version 7 and later
- Red Hat Enterprise Linux version 8 and later
- Red Hat Enterprise Linux version 9 and later

Red Hat Application Services products (formerly Red Hat Middleware)

- Red Hat JBoss BRMS version 5.0.1 and later, version 6.0.0 and later (also known as Red Hat Decision Manager, and currently part of Red Hat Process Automation Manager)
- JBoss Enterprise Web Server version 1 and later; Red Hat JBoss Web Server 3.0.1 and later
- Red Hat JBoss Enterprise Application Platform version 4.2 and later, version 4.3 and later, version 5 and later, version 6 and later, version 7 and later
- Red Hat Fuse version 6.0 and later

Red Hat Ansible Automation Platform

- Ansible Automation Platform version 2 and later

Red Hat OpenShift Container Platform

- Red Hat OpenShift Container Platform version 4 and later

Red Hat Advanced Cluster Security for Kubernetes

- Red Hat Advanced Cluster Security for Kubernetes version 4 and later

Red Hat Advanced Cluster Management for Kubernetes

- Red Hat Advanced Cluster Management for Kubernetes version 2 and later

1.3. IS DISCOVERY RIGHT FOR ME?

Discovery is intended to help you find and understand your Red Hat product inventory, including unknown product usage across complex networks. The reports generated by Discovery are best understood through your partnership with a Red Hat Solution Architect (SA) or Technical Account Manager (TAM) or through the analysis and assistance supplied by the Subscription Education and Awareness Program (SEAP).

Although you can install and use Discovery independently and then generate and view report data, the Discovery documentation does not provide any information to help you interpret report results. In addition, although Red Hat Support can provide some basic assistance related to installation and usage of Discovery, the support team does not provide any assistance to help you understand the reports.

The Discovery tool does not automatically share data directly with Red Hat. Instead, you choose whether to prepare and send report data to Red Hat for ingestion by Red Hat tools and services. You can use the Discovery tool locally to scan your network for the Red Hat products that Discovery currently supports and then use the generated reports for your own internal purposes.

CHAPTER 2. ACCESSING THE DISCOVERY USER INTERFACE

You access the Discovery graphical user interface through a browser.

Learn more

To learn more about the requirements and steps to log in to and out of the Discovery graphical user interface, see the following information:

- Logging in to the Discovery user interface
- Logging out of the Discovery user interface

2.1. LOGGING IN TO THE DISCOVERY USER INTERFACE

To log in to the Discovery user interface, you need the IP address of the system where the Discovery server is installed, the port number for the connection if the default port was changed during server installation, and the server administrator username and password to use when logging in. If you do not have this information, contact the administrator who installed the Discovery server.

Prerequisites

- To use the Discovery graphical user interface, the system on which you want to run the user interface must be able to communicate with the system on which the Discovery server is installed.

Procedure

1. In a browser, enter the URL for the Discovery server in the following format: **https://*IPaddress*:*server_port***, where ***IPaddress*** is the IP address of the Discovery server and ***server_port*** is the exposed server port.
   The following examples show two different ways to enter the URL, based on the system that you are logging in from and whether the default port is used:

   - If you log in from the system where the server is installed and the default port **9443** is used, you can use the loopback address (also known as localhost) as the IP address, as shown in the following example:

     ```
     https://127.0.0.1:9443
     ```

   - If you log in from a system that is remote from the server, the server is running on the IP address **192.0.2.0**, and the default port was changed during installation to **8443**, you would log in as shown in the following example:

     ```
     https://192.0.2.0:8443
     ```

   After you enter the URL for the server, the Discovery login page displays.

2. On the login page, enter the username and password for the Discovery server administrator account and then click **Log in** to log in to the server.

Verification steps

If this is the first time that you have logged in to Discovery, the Welcome page displays. You can begin by adding sources and credentials that can be used in scans. If you have previously logged in to

Discovery, the Welcome page is skipped and you can interact with your previously created sources, credentials, and scans.

2.2. LOGGING OUT OF THE DISCOVERY USER INTERFACE

Procedure

1. In the application toolbar, click the person icon or your username.
2. Click **Logout**.

CHAPTER 3. ADDING SOURCES AND CREDENTIALS

To prepare Discovery to run scans, you must add the parts of your IT infrastructure that you want to scan as one or more sources. You must also add the authentication information, such as a username and password or SSH key, that is required to access those sources as one or more credentials. Because of differing configuration requirements, you add sources and credentials according to the type of source that you are going to scan.

Learn more

As part of the general process of adding sources and credentials that encompass the different parts of your IT infrastructure, you might need to complete a number of tasks.

Add network sources and credentials to scan assets such as physical machines, virtual machines, or containers in your network. To learn more, see the following information:

- Adding Network sources and credentials

Add satellite sources and credentials to scan your deployment of Red Hat Satellite Server to find the assets that it manages. To learn more, see the following information:

- Adding Satellite sources and credentials

Add vcenter sources and credentials to scan your deployment of vCenter Server to find the assets that it manages. To learn more, see the following information:

- Adding vCenter sources and credentials

Add OpenShift sources and credentials to scan your deployment of Red Hat OpenShift Container Platform clusters. To learn more, see the following information:

- Adding OpenShift sources and credentials

Add Ansible sources and credentials to scan your deployment of Ansible Automation Platform to find the secured clusters that it manages. To learn more, see the following information:

- Adding Ansible sources and credentials

Add RHACS sources and credentials to scan your deployment of Red Hat Advanced Cluster Security for Kubernetes to find the secured clusters that RHACS manages. To learn more, see the following information:

- Adding RHACS sources and credentials

3.1. ADDING NETWORK SOURCES AND CREDENTIALS

To run a scan on one or more of the physical machines, virtual machines, or containers on your network, you must add a source that identifies each of the assets to scan. Then you must add credentials that contain the authentication data to access each asset.

Learn more

Add one or more network sources and credentials to provide the information needed to scan the assets in your network. To learn more, see the following information:

- To add a network source, see Adding network sources.

- To add a network credential, see Adding network credentials.

To learn more about sources and credentials and how Discovery uses them, see the following information:

- About sources and credentials

To learn more about how Discovery authenticates with assets on your network, see the following information. This information includes guidance about running commands with elevated privileges, a choice that you might need to make during network credential configuration:

- Network authentication
- Commands that are used in scans of remote network assets

3.1.1. Adding network sources

You can add sources from the initial Welcome page or from the Sources view.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Welcome page, click **Add Source**.
   - From the Sources view, click **Add**.

   The Add Source wizard opens.
2. On the Type page, select **Network Range** as the source type and click **Next**.
3. On the Credentials page, enter the following information.
   a. In the **Name** field, enter a descriptive name.
   b. In the **Search Addresses** field, enter one or more network identifiers separated by commas. You can enter hostnames, IP addresses, and IP ranges.
      - Enter hostnames as DNS hostnames, for example, **server1.example.com**.
      - Enter IP ranges in CIDR or Ansible notation, for example, **192.168.1.0/24** for CIDR notation or **192.168.1.[1:254]** for Ansible notation.
   c. Optional: In the **Port** field, enter a different port if you do not want a scan for this source to run on the default port 22.
   d. In the **Credentials** list, select the credentials that are required to access the network resources for this source. If a required credential does not exist, click the **Add a credential** icon to open the Add Credential wizard.
   e. If your network resources require the Ansible connection method to be the Python SSH implementation, Paramiko, instead of the default OpenSSH implementation, select the **Connect using Paramiko instead of OpenSSH** check box.
4. Click **Save** to save the source and then click **Close** to close the Add Source wizard.

3.1.2. Adding network credentials

You can add credentials from the Credentials view or from the Add Source wizard during the creation of a source. You might need to add several credentials to authenticate to all of the assets that are included in a single source.

Prerequisites

- If you want to use the SSH key authentication type for network credentials, each SSH private key that you are going to use must be copied into the directory that was mapped to **/sshkeys** during Discovery server installation. The default path for this directory is **"${HOME}"/.local/share/discovery/sshkeys**.
  For more information about the SSH keys that are available for use in the **/sshkeys** directory, or to request the addition of a key to that directory, contact the administrator who manages your Discovery server.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Credentials view, click **Add → Network Credential**.
   - From the Add Source wizard, click the **Add a credential** icon for the **Credentials** field.

   The Add Credential wizard opens.
2. In the **Credential Name** field, enter a descriptive name.
3. In the **Authentication Type** field, select the type of authentication that you want to use. You can select either **Username and Password** or **SSH Key**.
4. Enter the authentication data in the appropriate fields, based on the authentication type.
   - For username and password authentication, enter a username and password for a user. This user must have root-level access to your network or to the subset of your network that you want to scan. Alternatively, this user must be able to obtain root-level access with the selected become method.
   - For SSH key authentication, enter a username and the path to the SSH keyfile that is local to the Discovery server container. For example, if the keyfile is in the **"${HOME}"/.local/share/discovery/sshkeys** default path on the server, enter that path in the **SSH Key File** field. Entering a passphrase is optional.
5. Enter the become method for privilege elevation. Privilege elevation is required to run some commands during a network scan. Entering a username and password for the become method is optional.
6. Click **Save** to save the credential and close the Add Credential wizard.

3.1.3. About sources and credentials

To run a scan, you must configure data for two basic structures: sources and credentials. The type of source that you are going to inspect during the scan determines the type of data that is required for both source and credential configuration.

A *source* contains a single asset or a set of multiple assets that are to be inspected during the scan. You can configure four types of sources:

Network source

One or more physical machines, virtual machines, or containers. These assets can be expressed as hostnames, IP addresses, IP ranges, or subnets.

vCenter source

A vCenter Server systems management solution that is managing all or part of your IT infrastructure.

Satellite source

A Satellite systems management solution that is managing all or part of your IT infrastructure.

Red Hat OpenShift source

A Red Hat OpenShift Container Platform cluster that is managing all or part your Red Hat OpenShift Container Platform nodes and workloads.

Ansible source

An Ansible management solution that is managing your Ansible nodes and workloads.

Red Hat Advanced Cluster Security for Kubernetes source

A RHACS security platform solution that secures your Kubernetes environments.

When you are working with network sources, you determine how many individual assets you should group within a single source. Currently, you can add multiple assets to a source only for network sources. The following list contains some of the other factors that you should consider when you are adding sources:

- Whether assets are part of a development, testing, or production environment, and if demands on computing power and similar concerns are a consideration for those assets.
- Whether you want to scan a particular entity or group of entities more often because of internal business practices such as frequent changes to the installed software.

A *credential* contains data such as the username and password or SSH key of a user with sufficient authority to run the scan on all or part of the assets that are contained in that source. As with sources, credentials are configured as the network, vCenter, satellite, OpenShift, Ansible, or RHACS type. Typically, a network source might require multiple network credentials because it is expected that many credentials would be needed to access all of the assets in a broad IP range. Conversely, a vCenter or satellite source would typically use a single vCenter or satellite credential, as applicable, to access a particular system management solution server, and an OpenShift, Ansible, or RHACS source would use a single credential to access a single cluster.

You can add new sources from the Sources view and you can add new credentials from the Credentials view. You can also add new or select previously existing credentials during source creation. It is during source creation that you associate a credential directly with a source. Because sources and credentials must have matching types, any credential that you add during source creation shares the same type as the source. In addition, if you want to use an existing credential during source creation, the list of available credentials contains only credentials of the same type. For example, during network source creation, only network credentials are available for selection.

3.1.4. Network authentication

The Discovery server inspects the remote systems in a network scan by using the SSH remote connection capabilities of Ansible. When you add a network credential, you configure the SSH connection by using either a username and password or a username and SSH keyfile pair. If remote systems are accessed with SSH key authentication, you can also supply a passphrase.

Also during network credential configuration, you can enable a become method. The become method is used during a scan to elevate privileges. These elevated privileges are needed to run commands and

obtain data on the systems that you are scanning. For more information about the commands that do and do not require elevated privileges during a scan, see Commands that are used in scans of remote network assets.

3.1.4.1. Commands that are used in scans of remote network assets

When you run a network scan, Discovery must use the credentials that you provide to run certain commands on the remote systems in your network. Some of those commands must run with elevated privileges. This access is typically acquired through the use of the **sudo** command or similar commands. The elevated privileges are required to gather the types of facts that Discovery uses to build the report about your installed products.

Although it is possible to run a scan for a network source without elevated privileges, the results of that scan will be incomplete. The incomplete results from the network scan will affect the quality of the generated report for the scan.

The following information lists the commands that Discovery runs on remote hosts during a network scan. The information includes the basic commands that can run without elevated privileges and the commands that must run with elevated privileges to gather the most accurate and complete information for the report.

NOTE

In addition to the following commands, Discovery also depends on standard shell facilities, such as those provided by the **bash** shell.

3.1.4.1.1. Basic commands that do not need elevated privileges

The following commands do not require elevated privileges to gather facts during a scan:

- cat
- egrep
- sort
- uname
- ctime
- grep
- rpm
- virsh
- date
- id
- test
- whereis
- echo

- sed
- tune2fs
- xargs

3.1.4.1.2. Commands that need elevated privileges

The following commands require elevated privileges to gather facts during a scan. Each command includes a list of individual facts or categories of facts that Discovery attempts to find during a scan. These facts cannot be included in reports if elevated privileges are not available for that command.

- **awk**
- **cat**
- **chkconfig**
- **command**
- **df**
- **dirname**
- **dmidecode**
- **echo**
- **egrep**
- **fgrep**
- **find**
- **ifconfig**
- **ip**
- **java**
- **locate**
- **ls**
- **ps**
- **readlink**
- **sed**
- **sort**
- **stat**
- **subscription-manager**
- **systemctl**

- **tail**
- **test**
- **tr**
- **unzip**
- **virt-what**
- **xargs**
- **yum**

3.2. ADDING SATELLITE SOURCES AND CREDENTIALS

To run a scan on a Red Hat Satellite Server deployment, you must add a source that identifies the Satellite Server server to scan. Then you must add a credential that contains the authentication data to access that server.

Learn more

Add a satellite source and credential to provide the information needed to scan Satellite Server. To learn more, see the following information:

- To add a satellite source, see Adding satellite sources.
- To add a satellite credential, see Adding satellite credentials.

To learn more about sources and credentials and how Discovery uses them, see the following information:

- About sources and credentials

To learn more about how Discovery authenticates with your Satellite Server server, see the following information. This information includes guidance about certificate validation and SSL communication choices that you might need to make during satellite credential configuration.

- Satellite Server authentication

3.2.1. Adding satellite sources

You can add sources from the initial Welcome page or from the Sources view.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Welcome page, click **Add Source**.
   - From the Sources view, click **Add**.

   The Add Source wizard opens.
2. On the Type page, select **Satellite** as the source type and click **Next**.
3. On the Credentials page, enter the following information.

a. In the **Name** field, enter a descriptive name.

b. In the **IP Address or Hostname** field, enter the IP address or hostname of the Satellite server for this source. Enter a different port if you do not want a scan for this source to run on the default port 443. For example, if the IP address of the Satellite server is 192.0.2.15 and you want to change the port to 80, you would enter **192.0.2.15:80**.

c. In the **Credentials** list, select the credential that is required to access the Satellite server for this source. If a required credential does not exist, click the **Add a credential** icon to open the Add Credential wizard.

d. In the **Connection** list, select the SSL protocol to be used for a secure connection during a scan of this source.

NOTE

Satellite Server does not support the disabling of SSL. If you select the **Disable SSL** option, this option is ignored.

e. If you need to upgrade the SSL validation for the Satellite server to check for a verified SSL certificate from a certificate authority, select the **Verify SSL Certificate** check box.

4. Click **Save** to save the source and then click **Close** to close the Add Source wizard.

3.2.2. Adding satellite credentials

You can add credentials from the Credentials view or from the Add Source wizard during the creation of a source.

Procedure

1. Click the option to add a new credential based on your location:

   - From the Credentials view, click **Add → Satellite Credential**.
   - From the Add Source wizard, click the **Add a credential** icon for the **Credentials** field.

   The Add Credential wizard opens.

2. In the **Credential Name** field, enter a descriptive name.

3. Enter the username and password for a Satellite Server administrator.

4. Click **Save** to save the credential and close the Add Credential wizard.

3.2.3. About sources and credentials

To run a scan, you must configure data for two basic structures: sources and credentials. The type of source that you are going to inspect during the scan determines the type of data that is required for both source and credential configuration.

A *source* contains a single asset or a set of multiple assets that are to be inspected during the scan. You can configure four types of sources:

Network source

One or more physical machines, virtual machines, or containers. These assets can be expressed as hostnames, IP addresses, IP ranges, or subnets.

vCenter source

A vCenter Server systems management solution that is managing all or part of your IT infrastructure.

Satellite source

A Satellite systems management solution that is managing all or part of your IT infrastructure.

Red Hat OpenShift source

A Red Hat OpenShift Container Platform cluster that is managing all or part your Red Hat OpenShift Container Platform nodes and workloads.

Ansible source

An Ansible management solution that is managing your Ansible nodes and workloads.

Red Hat Advanced Cluster Security for Kubernetes source

A RHACS security platform solution that secures your Kubernetes environments.

When you are working with network sources, you determine how many individual assets you should group within a single source. Currently, you can add multiple assets to a source only for network sources. The following list contains some of the other factors that you should consider when you are adding sources:

- Whether assets are part of a development, testing, or production environment, and if demands on computing power and similar concerns are a consideration for those assets.
- Whether you want to scan a particular entity or group of entities more often because of internal business practices such as frequent changes to the installed software.

A *credential* contains data such as the username and password or SSH key of a user with sufficient authority to run the scan on all or part of the assets that are contained in that source. As with sources, credentials are configured as the network, vCenter, satellite, OpenShift, Ansible, or RHACS type. Typically, a network source might require multiple network credentials because it is expected that many credentials would be needed to access all of the assets in a broad IP range. Conversely, a vCenter or satellite source would typically use a single vCenter or satellite credential, as applicable, to access a particular system management solution server, and an OpenShift, Ansible, or RHACS source would use a single credential to access a single cluster.

You can add new sources from the Sources view and you can add new credentials from the Credentials view. You can also add new or select previously existing credentials during source creation. It is during source creation that you associate a credential directly with a source. Because sources and credentials must have matching types, any credential that you add during source creation shares the same type as the source. In addition, if you want to use an existing credential during source creation, the list of available credentials contains only credentials of the same type. For example, during network source creation, only network credentials are available for selection.

3.2.4. Satellite Server authentication

For a satellite scan, the connectivity and access to Satellite Server derives from basic authentication (username and password) that is encrypted over HTTPS. By default, the satellite scan runs with certificate validation and secure communication through the SSL (Secure Sockets Layer) protocol. During source creation, you can select from several different SSL and TLS (Transport Layer Security) protocols to use for the certificate validation and secure communication.

You might need to adjust the level of certificate validation to connect properly to the Satellite server during a scan. For example, your Satellite server might use a verified SSL certificate from a certificate authority. During source creation, you can upgrade SSL certificate validation to check for that

certificate during a scan of that source. Conversely, your Satellite server might use self-signed certificates. During source creation, you can leave the SSL validation at the default so that a scan of that source does not check for a certificate. This choice, to leave the option at the default for a self-signed certificate, could possibly avoid scan errors.

Although the option to disable SSL is currently available in the interface, Satellite Server does not support the disabling of SSL. If you select the **Disable SSL** option when you create a satellite source, this option is ignored.

3.3. ADDING VCENTER SOURCES AND CREDENTIALS

To run a scan on a vCenter Server deployment, you must add a source that identifies the vCenter Server server to scan. Then you must add a credential that contains the authentication data to access that server.

Learn more

Add a vcenter source and credential to provide the information needed to scan vCenter Server. To learn more, see the following information:

- To add a vcenter source, see Adding vcenter sources.
- To add a vcenter credential, see Adding vcenter credentials.

To learn more about sources and credentials and how Discovery uses them, see the following information:

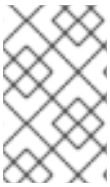
- About sources and credentials

To learn more about how Discovery authenticates with your vCenter Server server, see the following information. This information includes guidance about certificate validation and SSL communication choices that you might need to make during vcenter credential configuration:

- vCenter Server authentication

3.3.1. Adding vcenter sources

You can add sources from the initial Welcome page or from the Sources view.



NOTE

A vCenter source is only compatible with a vCenter deployment. You cannot use this source to scan other virtualization infrastructures, even those that are supported by Red Hat.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Welcome page, click **Add Source**.
   - From the Sources view, click **Add**.

   The Add Source wizard opens.
2. On the Type page, select **vCenter Server** as the source type and click **Next**.

3. On the Credentials page, enter the following information:

    a. In the **Name** field, enter a descriptive name.

    b. In the **IP Address or Hostname** field, enter the IP address or hostname of the vCenter Server for this source. Enter a different port if you do not want a scan for this source to run on the default port 443. For example, if the IP address of the vCenter Server is 192.0.2.15 and you want to change the port to 80, you would enter **192.0.2.15:80**.

    c. In the **Credentials** list, select the credential that is required to access the vCenter Server for this source. If a required credential does not exist, click the **Add a credential** icon to open the Add Credential wizard.

    d. In the **Connection** list, select the SSL protocol to be used for a secure connection during a scan of this source. Select **Disable SSL** to disable secure communication during a scan of this source.

    e. If you need to upgrade the SSL validation for the vCenter Server to check for a verified SSL certificate from a certificate authority, select the **Verify SSL Certificate** check box.

4. Click **Save** to save the source and then click **Close** to close the Add Source wizard.

3.3.2. Adding vcenter credentials

You can add credentials from the Credentials view or from the Add Source wizard during the creation of a source.

Procedure

1. Click the option to add a new credential based on your location:

    - From the Credentials view, click **Add → VCenter Credential**.
    - From the Add Source wizard, click the **Add a credential** icon for the **Credentials** field.

    The Add Credential wizard opens.

2. In the **Credential Name** field, enter a descriptive name.

3. Enter the username and password for a vCenter Server administrator.

4. Click **Save** to save the credential and close the Add Credential wizard.

3.3.3. About sources and credentials

To run a scan, you must configure data for two basic structures: sources and credentials. The type of source that you are going to inspect during the scan determines the type of data that is required for both source and credential configuration.

A *source* contains a single asset or a set of multiple assets that are to be inspected during the scan. You can configure four types of sources:

Network source

One or more physical machines, virtual machines, or containers. These assets can be expressed as hostnames, IP addresses, IP ranges, or subnets.

vCenter source

A vCenter Server systems management solution that is managing all or part of your IT infrastructure.

Satellite source

A Satellite systems management solution that is managing all or part of your IT infrastructure.

Red Hat OpenShift source

A Red Hat OpenShift Container Platform cluster that is managing all or part your Red Hat OpenShift Container Platform nodes and workloads.

Ansible source

An Ansible management solution that is managing your Ansible nodes and workloads.

Red Hat Advanced Cluster Security for Kubernetes source

A RHACS security platform solution that secures your Kubernetes environments.

When you are working with network sources, you determine how many individual assets you should group within a single source. Currently, you can add multiple assets to a source only for network sources. The following list contains some of the other factors that you should consider when you are adding sources:

- Whether assets are part of a development, testing, or production environment, and if demands on computing power and similar concerns are a consideration for those assets.
- Whether you want to scan a particular entity or group of entities more often because of internal business practices such as frequent changes to the installed software.

A *credential* contains data such as the username and password or SSH key of a user with sufficient authority to run the scan on all or part of the assets that are contained in that source. As with sources, credentials are configured as the network, vCenter, satellite, OpenShift, Ansible, or RHACS type. Typically, a network source might require multiple network credentials because it is expected that many credentials would be needed to access all of the assets in a broad IP range. Conversely, a vCenter or satellite source would typically use a single vCenter or satellite credential, as applicable, to access a particular system management solution server, and an OpenShift, Ansible, or RHACS source would use a single credential to access a single cluster.

You can add new sources from the Sources view and you can add new credentials from the Credentials view. You can also add new or select previously existing credentials during source creation. It is during source creation that you associate a credential directly with a source. Because sources and credentials must have matching types, any credential that you add during source creation shares the same type as the source. In addition, if you want to use an existing credential during source creation, the list of available credentials contains only credentials of the same type. For example, during network source creation, only network credentials are available for selection.

3.3.4. vCenter Server authentication

For a vcenter scan, the connectivity and access to vCenter Server derives from basic authentication (username and password) that is encrypted over HTTPS. By default, the vcenter scan runs with certificate validation and secure communication through the SSL (Secure Sockets Layer) protocol. During source creation, you can select from several different SSL and TLS (Transport Layer Security) protocols to use for the certificate validation and secure communication.

You might need to adjust the level of certificate validation to connect properly to the vCenter server during a scan. For example, your vCenter server might use a verified SSL certificate from a certificate authority. During source creation, you can upgrade SSL certificate validation to check for that certificate during a scan of that source. Conversely, your vCenter server might use self-signed

certificates. During source creation, you can leave the SSL validation at the default so that scan of that source does not check for a certificate. This choice, to leave the option at the default for a self-signed certificate, could possibly avoid scan errors.

You might also need to disable SSL as the method of secure communication during the scan if the vCenter server is not configured to use SSL communication for web applications. For example, your vCenter server might be configured to communicate with web applications by using HTTP with port 80. If so, then during source creation you can disable SSL communication for scans of that source.

3.4. ADDING OPENSHIFT SOURCES AND CREDENTIALS

To run a scan on a Red Hat OpenShift Container Platform deployment, you must add a source that identifies the Red Hat OpenShift Container Platform cluster to scan. Then you must add a credential that contains the authentication data to access that cluster.

Learn more

Add an OpenShift source and credential to provide the information needed to scan a Red Hat OpenShift Container Platform cluster. To learn more, see the following information:

- To add an OpenShift source, see Add an OpenShift source.
- To add an OpenShift credential, see Add an OpenShift credential.

To learn more about sources and credentials and how Discovery uses them, see the following information:

- About sources and credentials

To learn more about how Discovery authenticates with your Red Hat OpenShift Container Platform cluster, see the following information. This information includes guidance about certificate validation and SSL communication choices that you might need to make during OpenShift credential configuration:

- Red Hat OpenShift Container Platform authentication

3.4.1. Adding Red Hat OpenShift Container Platform sources

You can add sources from the initial Welcome page or from the Sources view.

Prerequisites

- You will need access to the Red Hat OpenShift Container Platform web console administrator perspective to get the API address and token values.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Welcome page, click **Add Source**.
   - From the Sources view, click **Add**.

   The Add Source wizard opens.
2. On the Type page, select **OpenShift** as the source type and click **Next**.

3. On the Credentials page, enter the following information:

    a. In the **Name** field, enter a descriptive name.

    b. In the **IP Address or Hostname** field, enter the Red Hat OpenShift Container Platform cluster API address for this source. You can find the cluster API address by viewing the overview details for the cluster in the web console

    c. In the **Credentials** list, select the credential that is required to access the cluster for this source. If a required credential does not exist, click the **Add a credential** icon to open the Add Credential wizard.

    d. In the **Connection** list, select the SSL protocol to be used for a secure connection during a scan of this source. Select **Disable SSL** to disable secure communication during a scan of this source.

    e. If you need to upgrade the SSL validation for the cluster to check for a verified SSL certificate from a certificate authority, select the **Verify SSL Certificate** check box.

4. Click **Save** to save the source and then click **Close** to close the Add Source wizard.

3.4.2. Adding Red Hat OpenShift Container Platform credentials

You can add credentials from the Credentials view or from the Add Source wizard during the creation of a source.

Prerequisites

- You will need access to the Red Hat OpenShift Container Platform web console administrator perspective to get the API address and token values.

Procedure

1. Click the option to add a new credential based on your location:

    - From the Credentials view, click **Add → OpenShift**.
    - From the Add Source wizard, click the **Add a credential** icon for the **Credentials** field.

    The Add Credential wizard opens.

2. In the **Credential Name** field, enter a descriptive name.

3. Enter the API token for the Red Hat OpenShift Container Platform cluster from your Administrator console. You can find the API token by clicking your username in the console, clicking the **Display Token** option and copying the value displayed for **Your API token is**.

4. Click **Save** to save the credential and close the Add Credential wizard.

3.4.3. About sources and credentials

To run a scan, you must configure data for two basic structures: sources and credentials. The type of source that you are going to inspect during the scan determines the type of data that is required for both source and credential configuration.

A *source* contains a single asset or a set of multiple assets that are to be inspected during the scan. You can configure four types of sources:

Network source

One or more physical machines, virtual machines, or containers. These assets can be expressed as hostnames, IP addresses, IP ranges, or subnets.

vCenter source

A vCenter Server systems management solution that is managing all or part of your IT infrastructure.

Satellite source

A Satellite systems management solution that is managing all or part of your IT infrastructure.

Red Hat OpenShift source

A Red Hat OpenShift Container Platform cluster that is managing all or part your Red Hat OpenShift Container Platform nodes and workloads.

Ansible source

An Ansible management solution that is managing your Ansible nodes and workloads.

Red Hat Advanced Cluster Security for Kubernetes source

A RHACS security platform solution that secures your Kubernetes environments.

When you are working with network sources, you determine how many individual assets you should group within a single source. Currently, you can add multiple assets to a source only for network sources. The following list contains some of the other factors that you should consider when you are adding sources:

- Whether assets are part of a development, testing, or production environment, and if demands on computing power and similar concerns are a consideration for those assets.
- Whether you want to scan a particular entity or group of entities more often because of internal business practices such as frequent changes to the installed software.

A *credential* contains data such as the username and password or SSH key of a user with sufficient authority to run the scan on all or part of the assets that are contained in that source. As with sources, credentials are configured as the network, vCenter, satellite, OpenShift, Ansible, or RHACS type. Typically, a network source might require multiple network credentials because it is expected that many credentials would be needed to access all of the assets in a broad IP range. Conversely, a vCenter or satellite source would typically use a single vCenter or satellite credential, as applicable, to access a particular system management solution server, and an OpenShift, Ansible, or RHACS source would use a single credential to access a single cluster.

You can add new sources from the Sources view and you can add new credentials from the Credentials view. You can also add new or select previously existing credentials during source creation. It is during source creation that you associate a credential directly with a source. Because sources and credentials must have matching types, any credential that you add during source creation shares the same type as the source. In addition, if you want to use an existing credential during source creation, the list of available credentials contains only credentials of the same type. For example, during network source creation, only network credentials are available for selection.

3.4.4. Red Hat OpenShift Container Platform authentication

For a OpenShift scan, the connectivity and access to OpenShift cluster API address derives from basic authentication with a cluster API address and an API token that is encrypted over HTTPS. By default, the OpenShift scan runs with certificate validation and secure communication through the SSL (Secure

Sockets Layer) protocol. During source creation, you can select from several different SSL and TLS (Transport Layer Security) protocols to use for the certificate validation and secure communication.

You might need to adjust the level of certificate validation to connect properly to the Red Hat OpenShift Container Platform cluster API address during a scan. For example, your OpenShift cluster API address might use a verified SSL certificate from a certificate authority. During source creation, you can upgrade SSL certificate validation to check for that certificate during a scan of that source. Conversely, your cluster API address might use self-signed certificates. During source creation, you can leave the SSL validation at the default so that scan of that source does not check for a certificate. This choice, to leave the option at the default for a self-signed certificate, could possibly avoid scan errors.

You might also need to disable SSL as the method of secure communication during the scan if the OpenShift cluster API address is not configured to use SSL communication for web applications. For example, your OpenShift server might be configured to communicate with web applications by using HTTP with port 80. If so, then during source creation you can disable SSL communication for scans of that source.

3.5. ADDING ANSIBLE SOURCES AND CREDENTIALS

To run a scan on a Ansible deployment, you must add a source that identifies the Ansible Automation Platform to scan. Then, you must add a credential that contains the authentication data to access that cluster.

Learn more

Add an Ansible source and credential to provide the information needed to scan your Ansible Automation Platform deployment. To learn more, see the following information:

- To add an Ansible source, see Add an Ansible source .
- To add an Ansible credential, see Add an Ansible credential .

To learn more about sources and credentials and how Discovery uses them, see the following information:

- About sources and credentials

To learn more about how Discovery authenticates with your Ansible deployment, see the following information. This information includes guidance about certificate validation and SSL communication choices that you might need to make during Ansible credential configuration:

- Ansible Automation Platform

3.5.1. Adding Red Hat Ansible Automation Platform sources

You can add sources from the initial Welcome page or from the Sources view.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Welcome page, click **Add Source**.
   - From the Sources view, click **Add Source**.

   The Add Source wizard opens.

2. On the Type page, select **Ansible Controller** as the source type and click **Next**.
3. On the Credentials page, enter the following information:
    a. In the **Name** field, enter a descriptive name.
    b. In the **IP Address or Hostname** field, enter the Ansible host IP address for this source. You can find the host IP address by viewing the overview details for the controller in the portal.
    c. In the **Credentials** list, select the credential that is required to access the cluster for this source. If a required credential does not exist, click the **Add a credential** icon to open the Add Credential wizard.
    d. In the **Connection** list, select the SSL protocol to be used for a secure connection during a scan of this source. Select **Disable SSL** to disable secure communication during a scan of this source.
    e. If you need to upgrade the SSL validation for the cluster to check for a verified SSL certificate from a certificate authority, select the **Verify SSL Certificate** check box.
4. Click **Save** to save the source and then click **Close** to close the Add Source wizard.

3.5.2. Adding Red Hat Ansible Automation Platform credentials

You can add credentials from the Credentials view or from the Add Source wizard during the creation of a source.

Procedure

1. Click the option to add a new credential based on your location:
    - From the Credentials view, click **Add → Ansible Credential**.
    - From the Add Source wizard, click the **Add a credential** icon for the **Credentials** field.

    The Add Credential wizard opens.
2. In the **Credential Name** field, enter a descriptive name.
3. In the **User Name** field, enter the username for your Ansible Controller instance.
4. In the **Password** field, enter the password for your Ansible Controller instance.
5. Click **Save** to save the credential. The Add credential wizard closes.

3.5.3. About sources and credentials

To run a scan, you must configure data for two basic structures: sources and credentials. The type of source that you are going to inspect during the scan determines the type of data that is required for both source and credential configuration.

A *source* contains a single asset or a set of multiple assets that are to be inspected during the scan. You can configure four types of sources:

Network source

One or more physical machines, virtual machines, or containers. These assets can be expressed as hostnames, IP addresses, IP ranges, or subnets.

vCenter source

A vCenter Server systems management solution that is managing all or part of your IT infrastructure.

Satellite source

A Satellite systems management solution that is managing all or part of your IT infrastructure.

Red Hat OpenShift source

A Red Hat OpenShift Container Platform cluster that is managing all or part your Red Hat OpenShift Container Platform nodes and workloads.

Ansible source

An Ansible management solution that is managing your Ansible nodes and workloads.

Red Hat Advanced Cluster Security for Kubernetes source

A RHACS security platform solution that secures your Kubernetes environments.

When you are working with network sources, you determine how many individual assets you should group within a single source. Currently, you can add multiple assets to a source only for network sources. The following list contains some of the other factors that you should consider when you are adding sources:

- Whether assets are part of a development, testing, or production environment, and if demands on computing power and similar concerns are a consideration for those assets.
- Whether you want to scan a particular entity or group of entities more often because of internal business practices such as frequent changes to the installed software.

A *credential* contains data such as the username and password or SSH key of a user with sufficient authority to run the scan on all or part of the assets that are contained in that source. As with sources, credentials are configured as the network, vCenter, satellite, OpenShift, Ansible, or RHACS type. Typically, a network source might require multiple network credentials because it is expected that many credentials would be needed to access all of the assets in a broad IP range. Conversely, a vCenter or satellite source would typically use a single vCenter or satellite credential, as applicable, to access a particular system management solution server, and an OpenShift, Ansible, or RHACS source would use a single credential to access a single cluster.

You can add new sources from the Sources view and you can add new credentials from the Credentials view. You can also add new or select previously existing credentials during source creation. It is during source creation that you associate a credential directly with a source. Because sources and credentials must have matching types, any credential that you add during source creation shares the same type as the source. In addition, if you want to use an existing credential during source creation, the list of available credentials contains only credentials of the same type. For example, during network source creation, only network credentials are available for selection.

3.5.4. Ansible authentication

For a Ansible scan, the connectivity and access to Ansible host IP addresses derives from basic authentication with a host IP address and a password that is encrypted over HTTPS. By default, the Ansible scan runs with certificate validation and secure communication through the SSL (Secure Sockets Layer) protocol. During source creation, you can select from several different SSL and TLS (Transport Layer Security) protocols to use for the certificate validation and secure communication.

You might need to adjust the level of certificate validation to connect properly to the Ansible host IP address during a scan. For example, your Ansible host Ip address might use a verified SSL certificate from a certificate authority. During source creation, you can upgrade SSL certificate validation to check

for that certificate during a scan of that source. Conversely, your host IP address might use self-signed certificates. During source creation, you can leave the SSL validation at the default so that scan of that source does not check for a certificate. This choice, to leave the option at the default for a self-signed certificate, could possibly avoid scan errors.

You might also need to disable SSL as the method of secure communication during the scan if the Ansible host IP address is not configured to use SSL communication for web applications. For example, your Ansible host IP address might be configured to communicate with web applications by using HTTP with port 80. If so, then during source creation you can disable SSL communication for scans of that source.

3.6. ADDING RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES SOURCES AND CREDENTIALS

To run a scan on a Red Hat Advanced Cluster Security for Kubernetes (RHACS) deployment, you must add a source that identifies the RHACS instance to scan. Then you must add a credential that contains the authentication data to access that instance.

Learn more

Add a RHACS source and credential to provide the information needed to scan a RHACS instance. To learn more, see the following information:

- To add an RHACS source, see Add a RHACS source.
- To add an RHACS credential, see Add a RHACS credential.

To learn more about sources and credentials and how Discovery uses them, see the following information:

- About sources and credentials

To learn more about how Discovery authenticates with your Red Hat Advanced Cluster Security for Kubernetes instance, see the following information. This information includes guidance about certificate validation and SSL communication choices that you might need to make during RHACS credential configuration:

- Red Hat Advanced Cluster Security for Kubernetes

3.6.1. Adding Red Hat Advanced Cluster Security for Kubernetes sources

You can add sources from the initial Welcome page or from the Sources view.

Prerequisites

- You will need access to the Red Hat Advanced Cluster Security for Kubernetes (RHACS) portal to generate admin API token values.
- You will need either access to the RHACS portal to find the RHACS Central endpoint or access the RHACS Configuration Management Cloud Service instance details.

Procedure

1. Click the option to add a new credential based on your location:
    - From the Welcome page, click **Add Source**.

- From the Sources view, click **Add**.

The Add Source wizard opens.

2. On the Type page, select **RHACS** as the source type and click **Next**.
3. On the Credentials page, enter the following information:
   a. In the **Name** field, enter a descriptive name.
   b. In the **IP Address or Hostname** field, enter the Red Hat Advanced Cluster Security for Kubernetes Central address for this source.
      - You can find the address by viewing the network routes for the cluster if RHACS was deployed on OpenShift.
      - If RHACS was deployed on the cloud, you can find this information in the instance details.
   c. In the **Credentials** list, select the credential that is required to access the cluster for this source. If a required credential does not exist, click the **Add a credential** icon to open the Add Credential wizard.
   d. In the **Connection** list, select the SSL protocol to be used for a secure connection during a scan of this source. Select **Disable SSL** to disable secure communication during a scan of this source.
   e. If you need to upgrade the SSL validation for the cluster to check for a verified SSL certificate from a certificate authority, select the **Verify SSL Certificate** check box.
4. Click **Save** to save the source and then click **Close** to close the Add Source wizard.

3.6.2. Adding RHACS credentials

You can add credentials from the Credentials view or from the Add Source wizard during the creation of a source.

Prerequisites

- You will need access to the Red Hat Advanced Cluster Security for Kubernetes (RHACS) portal to generate admin API token values.
- You will need either access to the RHACS portal to find the RHACS Central endpoint or access the RHACS Configuration Management Cloud Service instance details.

Procedure

1. Click the option to add a new credential based on your location:
   - From the Credentials view, click **Add → RHACS**.
   - From the Add Source wizard, click the **Add a credential** icon for the **Credentials** field.

   The Add Credential wizard opens.
2. In the **Credential Name** field, enter a descriptive name.

3. Enter the API token for RHACS from yourRHACS portal. If you do not already have a token, you can generate a token on the RHACSConfiguration Management Cloud Service portal.

4. Click **Save** to save the credential and close the Add Credential wizard.

3.6.3. About sources and credentials

To run a scan, you must configure data for two basic structures: sources and credentials. The type of source that you are going to inspect during the scan determines the type of data that is required for both source and credential configuration.

A *source* contains a single asset or a set of multiple assets that are to be inspected during the scan. You can configure four types of sources:

Network source

One or more physical machines, virtual machines, or containers. These assets can be expressed as hostnames, IP addresses, IP ranges, or subnets.

vCenter source

A vCenter Server systems management solution that is managing all or part of your IT infrastructure.

Satellite source

A Satellite systems management solution that is managing all or part of your IT infrastructure.

Red Hat OpenShift source

A Red Hat OpenShift Container Platform cluster that is managing all or part your Red Hat OpenShift Container Platform nodes and workloads.

Ansible source

An Ansible management solution that is managing your Ansible nodes and workloads.

Red Hat Advanced Cluster Security for Kubernetes source

A RHACS security platform solution that secures your Kubernetes environments.

When you are working with network sources, you determine how many individual assets you should group within a single source. Currently, you can add multiple assets to a source only for network sources. The following list contains some of the other factors that you should consider when you are adding sources:

- Whether assets are part of a development, testing, or production environment, and if demands on computing power and similar concerns are a consideration for those assets.

- Whether you want to scan a particular entity or group of entities more often because of internal business practices such as frequent changes to the installed software.

A *credential* contains data such as the username and password or SSH key of a user with sufficient authority to run the scan on all or part of the assets that are contained in that source. As with sources, credentials are configured as the network, vCenter, satellite, OpenShift, Ansible, or RHACS type. Typically, a network source might require multiple network credentials because it is expected that many credentials would be needed to access all of the assets in a broad IP range. Conversely, a vCenter or satellite source would typically use a single vCenter or satellite credential, as applicable, to access a particular system management solution server, and an OpenShift, Ansible, or RHACS source would use a single credential to access a single cluster.

You can add new sources from the Sources view and you can add new credentials from the Credentials view. You can also add new or select previously existing credentials during source creation. It is during source creation that you associate a credential directly with a source. Because sources and credentials

must have matching types, any credential that you add during source creation shares the same type as the source. In addition, if you want to use an existing credential during source creation, the list of available credentials contains only credentials of the same type. For example, during network source creation, only network credentials are available for selection.

3.6.4. Red Hat Advanced Cluster Security for Kubernetes authentication

For a Red Hat Advanced Cluster Security for Kubernetes (RHACS) scan, the connectivity and access to the RHACS API derives from bearer token authentication with an API token that is encrypted over TLS (Transport Layer Security). By default, the RHACS scan runs with certificate validation and secure communication through the TLS protocol. During source creation, you can select from several different SSL (Secure Sockets Layer) and TLS protocols to use for the certificate validation and secure communication.

You might need to adjust the level of certificate validation to connect to the RHACS portal during a scan. For example, your RHACS instance might use a verified TLS certificate from a certificate authority. During source creation, you can upgrade TLS certificate validation to check for that certificate during a scan of that source. Conversely, your RHACS instance might use self-signed certificates. During source creation, you can leave the TLS validation at the default so that scan of that source does not check for a certificate. This choice, to leave the option at the default for a self-signed certificate, could possibly avoid scan errors.

You might also need to disable TSL as the method of secure communication during the scan if the RHACS instance is not configured to use TSL communication for web applications. For example, your RHACS instance might be configured to communicate with web applications by using HTTP with port 80. If so, then during source creation you can disable TSL communication for scans of that source.

CHAPTER 4. RUNNING AND MANAGING SCANS

After you add sources and credentials for the parts of your IT infrastructure that you want to scan, you can create and run scans. When you create a scan, you can choose to scan a single source or combine multiple sources from different source types. You can also choose whether to run a standard scan for products that are installed with default installation processes and locations or to run a deep scan if products might be installed with nonstandard processes or locations.

NOTE

Currently you cannot combine an OpenShift, Ansible, or RHACS scan with any other type of source in a scan. However, a single OpenShift, Ansible, or RHACS scan can contain multiple sources of the same type, each of which is associated with a single cluster only.

After a scan is created, you can run that scan multiple times. Each instance of that scan is saved as a scan job.

Learn more

To learn more about running a standard scan that does not use deep scanning for products, see the following information:

- Running and managing standard scans

To learn more about running a deep scan, a scan that can find products that might have been installed with a nonstandard process or in a nonstandard location, see the following information:

- Running and managing deep scans

4.1. RUNNING AND MANAGING STANDARD SCANS

After you add sources and credentials for the parts of your IT infrastructure that you want to scan, you can begin running scans. In most situations, you can run a standard scan to find the environment and product data that is required to report on your Red Hat products.

Learn more

Run a standard scan to find products in standard locations. To learn more, see the following information:

- Running standard scans

When you begin running scans, there are several tasks that you can do to manage your scans. These tasks include updating the data for a scan by running a new scan job and managing active scans by pausing, resuming, and canceling. When you are finished with a scan, you can delete it. To learn more, see the following information:

- Running a new scan job
- Pausing, resuming, and canceling scans
- Deleting scans

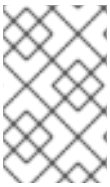
To learn more about how scans and scan jobs work, including how a scan job is processed by Discovery and the states a scan job moves through during its life cycle, see the following information:

- About scans and scan jobs

- Scan job processing
- Scan job life cycle

4.1.1. Running standard scans

You can run a new scan from the Sources view. You can run a scan for a single source or select multiple sources to combine into a single scan. Each time that you use the Sources view to run a scan, you are prompted to save it as a new scan.



NOTE

Currently you cannot combine an OpenShift, Ansible, or RHACS scan with any other type of source in a scan. However, a single OpenShift, Ansible, or RHACS scan can contain multiple sources of the same type, each of which is associated with a single cluster only.

After you run a scan for the first time, the scan is saved to the Scans view. From that view, you can run that scan again to update its data. Each time that you run a scan from the Scans view, it is saved as a new scan job for that scan.

Prerequisites

- To run a scan, you must first add the sources that you want to scan and the credentials to access those sources.

Procedure

1. From the Sources view, select one or more sources. You can select sources of different types to combine them into a single scan.
2. Click the **Scan** button that is appropriate for the selected sources:
   - For a single source, click **Scan** on the row for that source. Selecting the check box for the source is optional.
   - If you selected multiple sources, click **Scan** in the toolbar.

   The Scan wizard opens.
3. In the **Name** field, enter a descriptive name for the scan.
4. If you want to change the default number of maximum concurrent scans, set a new value in the **Maximum concurrent scans** field. This value is the maximum number of physical machines or virtual machines that are scanned in parallel during a scan.
5. To use the default scanning process, allow the **Deep scan for these products**check boxes to remain in the default, cleared state.
6. To begin the scan process, click **Scan**.

Verification steps

When the scan process begins, a notification displays in the Sources view. The running scan also displays in the Scans view, with a message about the progress of the scan.

4.1.2. Running a new scan job

After you name a scan and run it for the first time, it is added to the Scans view. You can then run a new instance of that scan, known as a scan job, to update the data that is gathered for that scan.

Procedure

1. From the Scans view, click the **Run Scan** icon in the scan details.

NOTE

In the scan details, if the most recent scan job did not complete successfully, this icon is labeled **Retry Scan**.

Verification steps

When the scan process begins, a notification displays with a message about the progress of the scan. If you want to view a completed scan, you can view the scan details and expand **Previous** to view all previous scan jobs.

4.1.3. Pausing, resuming, and canceling scans

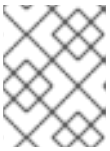
As you begin running scans, you might need to stop a scan job that is currently running. There might be various business reasons that require you to do this, for example, the need to do an emergency fix due to an alert from your IT health monitoring system or the need to run a higher priority scan that consumes more CPU resources than a lower priority scan that is currently running.

You can stop a scan job by either pausing it or canceling it. You can resume a paused scan job, but you cannot resume a canceled scan job.

Procedure

To pause a scan job that is running:

1. From the Scans view, find the scan that contains the scan job that you want to pause.
2. Click **Pause Scan**.



NOTE

If you have multiple scans running at the same time, it might take several moments after starting a scan for the **Pause Scan** icon to appear.

To resume a scan job that is paused:

1. From the Scans view, find the scan that contains the scan job that you want to resume.
2. Click **Resume Scan**.

To cancel a scan job that is running:

1. From the Scans view, find the scan that contains the scan job that you want to cancel.
2. Click **Cancel Scan**.

4.1.4. Deleting scans

Deleting a scan is a nonreversible action that deletes the scan and all scan jobs for that scan. Deleted scans cannot be retrieved.

Prerequisites

- To delete a scan, a scan needs to be run first for it to display in the **Scans** navigation.

Procedure

1. From the navigation, click **Scans.**
2. Find the row that contains the scan that you would like to delete.
3. Click the **Delete** icon for that row.

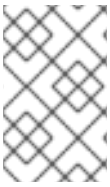
Result

- Your scan is deleted.

4.1.5. About scans and scan jobs

After you create sources and credentials, you can create scans. A *scan* is an object that groups sources into a unit that can be inspected, or scanned, in a reproducible way. Each time that you run a saved scan, that instance is saved as a *scan job*. The output of a scan job is a *report*, the collection of facts gathered for all IT resources that are contained in that source.

A scan includes at least one source and the credentials that were associated with that source at source creation time. When the scan job runs, it uses the provided credentials to contact the assets contained in the source and then it inspects the assets to gather facts about those assets for the report. You can add multiple sources to a single scan, including a combination of different types of sources into a single scan.



NOTE

Currently, you cannot combine a OpenShift source with any other type of source in a scan. However, a single OpenShift scan can contain multiple OpenShift sources, each of which is associated with a single cluster only.

4.1.6. Scan job processing

A scan job moves through two phases, or tasks, while it is being processed. These two tasks are the connection task and the inspection task.

4.1.6.1. Scan job connection and inspection tasks

The first task that runs during a scan job is a connection task. The *connection task* determines the ability to connect to the source and finds the number of systems that can be inspected for the defined source. The second task that runs is an inspection task. The *inspection task* is the task that gathers data from each of the reachable systems in the defined source to output the scan results into a report.

If the scan is configured so that it contains several sources, then when the scan job runs, these two tasks are created for each source. First, all of the connection tasks for all of the sources run to establish

connections to the sources and find the systems that can be inspected. Then all of the inspection tasks for all of the sources run to inspect the contents of the reachable systems that are contained in the sources.

4.1.6.2. How these tasks are processed

When the scan job runs the connection task for a source, it attempts to connect to the network, the server, the cluster, or the instance used. If the connection fails, then the connection task fails. For a network scan, if the network is not reachable or the credentials are invalid, the connection task reports zero (0) successful systems. If only some of the systems for a network scan are reachable, the connection task reports success on the systems that are reachable, and the connection task does not fail.

You can view information about the status of the connection task in the Scans view. The row for a scan displays the connection task results as the number of successful system connections for the most recent scan job. You can also expand the previous scan jobs to see the connection task results for a previous scan job.

When the scan job runs the inspection task for a source, it checks the state of the connection task. If the connection task shows a failed state or if there are zero (0) successful connections, the scan job transitions to the failed state. However, if the connection task reports at least one successful connection, the inspection task continues. The results for the scan job then show success and failure data for each individual system. If the inspection task is not able to gather results from the successful systems, or if another unexpected error occurs during the inspection task, then the scan job transitions to the failed state.

If a scan contains multiple sources, each source has its own connection and inspection tasks. These tasks are processed independently from the tasks for the other sources. If any task for any of the sources fails, the scan job transitions to the failed state. The scan job transitions to the completed state only if all scan job tasks for all sources complete successfully.

If a scan job completes successfully, the data for that scan job is generated as a report. In the Scans view, you can download the report for each successful scan job.

4.1.7. Scan job life cycle

A *scan job*, or individual instance of a scan, moves through several states during its life cycle.

When you start a scan, a scan job is created and the scan job is in the *created* state. The scan job is then queued for processing and the scan job transitions to the *pending* state. Scan jobs run serially, in the order that they are started.

As the Discovery server reaches a specific scan job in the queue, that scan job transitions from the *pending* state to the *running* state as the processing of that scan job begins. If the scan process completes successfully, the scan job transitions to the *completed* state and the scan job produces results that can be viewed in a report. If the scan process results in an error that prevents successful completion of the scan, the scan job halts and the scan job transitions to the *failed* state. An additional status message for the failed scan contains information to help determine the cause of the failure.

Other states for a scan job result from user action that is taken on the scan job. You can pause or cancel a scan job while it is pending or running. A scan job in the *paused* state can be resumed. A scan job in the *canceled* state cannot be resumed.

4.2. RUNNING AND MANAGING DEEP SCANS

After you add sources and credentials for the parts of your IT infrastructure that you want to scan, you can begin running scans. In a few situations, running standard scans is not sufficient to find the environment and product data that is required to report on your Red Hat products.

By default, Discovery searches for and fingerprints products by using known metadata that relates to those products. However, it is possible that you have installed these products with a process or in an installation location that makes the search and fingerprinting algorithms less effective. In that case, you need to use deep scanning to find those products.

Learn more

Run a deep scan to find products in nonstandard locations. To learn more, see the following information:

- Running scans with deep scanning

When you begin running scans, there are several tasks that you can do to manage your scans. These tasks include updating the data for a scan by running a new scan job and managing active scans by pausing, resuming, and canceling. When you are finished with a scan, you can delete it. To learn more, see the following information:

- Running a new scan job
- Pausing, resuming, and canceling scans
- Deleting scans

To learn more about how scans and scan jobs work, including how a scan job is processed by Discovery and the states a scan job moves through during its life cycle, see the following information:

- About scans and scan jobs
- Scan job processing
- Scan job life cycle

4.2.1. Running scans with deep scanning

You can run a new scan from the Sources view. You can run a scan for a single source or select multiple sources to combine into a single scan. As part of the scan configuration, you might choose to use the deep scanning process to search for products in nonstandard locations.

NOTE

Currently you cannot combine a OpenShift, Ansible or RHACS scan with any other type of source in a scan. However, a single OpenShift, Ansible or RHACS scan can contain multiple OpenShift, Ansible or RHACS sources, each of which is associated with a single cluster only.

The deep scanning process uses the **find** command, so the search process could be CPU resource intensive for the systems that are being scanned. Therefore, you should use discretion when selecting a deep scan for systems that require continuous availability, such as production systems.

After you run a scan for the first time, the scan is saved to the Scans view. From that view, you can run the scan again to update its data.

Prerequisites

- To run a scan, you must first add the sources that you want to scan and the credentials to access those sources.

Procedure

1. From the Sources view, select one or more sources. You can select sources of different types to combine them into a single scan.
2. Click the **Scan** button that is appropriate for the selected sources:
   - For a single source, click **Scan** on the row for that source. Selecting the check box for the source is optional.
   - If you selected multiple sources, click **Scan** in the toolbar.

   The Scan wizard opens.
3. In the **Name** field, enter a descriptive name for the scan.
4. If you want to change the default number of maximum concurrent scans, set a new value in the **Maximum concurrent scans** field. This value is the maximum number of physical machines or virtual machines that are scanned in parallel during a scan.
5. To use the deep scanning process on one or more products, supply the following information:
   - Select the applicable **Deep scan for these products**check boxes.
   - Optionally, enter the directories that you want Discovery to scan. The default directories that are used in a deep scan are the /, /**opt**, /**app**, /**home**, and /**usr** directories.
6. To begin the scan process, click **Scan**.

Verification steps

When the scan process begins, a notification displays in the Sources view. The running scan also displays in the Scans view, with a message about the progress of the scan.

4.2.2. Running a new scan job

After you name a scan and run it for the first time, it is added to the Scans view. You can then run a new instance of that scan, known as a scan job, to update the data that is gathered for that scan.

Procedure

1. From the Scans view, click the **Run Scan** icon in the scan details.

NOTE

In the scan details, if the most recent scan job did not complete successfully, this icon is labeled **Retry Scan**.

Verification steps

When the scan process begins, a notification displays with a message about the progress of the scan. If you want to view a completed scan, you can view the scan details and expand **Previous** to view all previous scan jobs.

4.2.3. Pausing, resuming, and canceling scans

As you begin running scans, you might need to stop a scan job that is currently running. There might be various business reasons that require you to do this, for example, the need to do an emergency fix due to an alert from your IT health monitoring system or the need to run a higher priority scan that consumes more CPU resources than a lower priority scan that is currently running.

You can stop a scan job by either pausing it or canceling it. You can resume a paused scan job, but you cannot resume a canceled scan job.

Procedure

To pause a scan job that is running:

1. From the Scans view, find the scan that contains the scan job that you want to pause.
2. Click **Pause Scan**.

NOTE

If you have multiple scans running at the same time, it might take several moments after starting a scan for the **Pause Scan** icon to appear.

To resume a scan job that is paused:

1. From the Scans view, find the scan that contains the scan job that you want to resume.
2. Click **Resume Scan**.

To cancel a scan job that is running:

1. From the Scans view, find the scan that contains the scan job that you want to cancel.
2. Click **Cancel Scan**.

4.2.4. Deleting scans

Deleting a scan is a nonreversible action that deletes the scan and all scan jobs for that scan. Deleted scans cannot be retrieved.

Prerequisites

- To delete a scan, a scan needs to be run first for it to display in the **Scans** navigation.

Procedure

1. From the navigation, click **Scans.**
2. Find the row that contains the scan that you would like to delete.
3. Click the **Delete** icon for that row.

Result

- Your scan is deleted.

4.2.5. About scans and scan jobs

After you create sources and credentials, you can create scans. A *scan* is an object that groups sources into a unit that can be inspected, or scanned, in a reproducible way. Each time that you run a saved scan, that instance is saved as a *scan job*. The output of a scan job is a *report*, the collection of facts gathered for all IT resources that are contained in that source.

A scan includes at least one source and the credentials that were associated with that source at source creation time. When the scan job runs, it uses the provided credentials to contact the assets contained in the source and then it inspects the assets to gather facts about those assets for the report. You can add multiple sources to a single scan, including a combination of different types of sources into a single scan.

NOTE

Currently, you cannot combine a OpenShift source with any other type of source in a scan. However, a single OpenShift scan can contain multiple OpenShift sources, each of which is associated with a single cluster only.

4.2.6. Scan job processing

A scan job moves through two phases, or tasks, while it is being processed. These two tasks are the connection task and the inspection task.

4.2.6.1. Scan job connection and inspection tasks

The first task that runs during a scan job is a connection task. The *connection task* determines the ability to connect to the source and finds the number of systems that can be inspected for the defined source. The second task that runs is an inspection task. The *inspection task* is the task that gathers data from each of the reachable systems in the defined source to output the scan results into a report.

If the scan is configured so that it contains several sources, then when the scan job runs, these two tasks are created for each source. First, all of the connection tasks for all of the sources run to establish connections to the sources and find the systems that can be inspected. Then all of the inspection tasks for all of the sources run to inspect the contents of the reachable systems that are contained in the sources.

4.2.6.2. How these tasks are processed

When the scan job runs the connection task for a source, it attempts to connect to the network, the server, the cluster, or the instance used. If the connection fails, then the connection task fails. For a network scan, if the network is not reachable or the credentials are invalid, the connection task reports zero (0) successful systems. If only some of the systems for a network scan are reachable, the connection task reports success on the systems that are reachable, and the connection task does not fail.

You can view information about the status of the connection task in the Scans view. The row for a scan displays the connection task results as the number of successful system connections for the most recent scan job. You can also expand the previous scan jobs to see the connection task results for a previous scan job.

When the scan job runs the inspection task for a source, it checks the state of the connection task. If the connection task shows a failed state or if there are zero (0) successful connections, the scan job transitions to the failed state. However, if the connection task reports at least one successful connection, the inspection task continues. The results for the scan job then show success and failure

data for each individual system. If the inspection task is not able to gather results from the successful systems, or if another unexpected error occurs during the inspection task, then the scan job transitions to the failed state.

If a scan contains multiple sources, each source has its own connection and inspection tasks. These tasks are processed independently from the tasks for the other sources. If any task for any of the sources fails, the scan job transitions to the failed state. The scan job transitions to the completed state only if all scan job tasks for all sources complete successfully.

If a scan job completes successfully, the data for that scan job is generated as a report. In the Scans view, you can download the report for each successful scan job.

4.2.7. Scan job life cycle

A *scan job*, or individual instance of a scan, moves through several states during its life cycle.

When you start a scan, a scan job is created and the scan job is in the *created* state. The scan job is then queued for processing and the scan job transitions to the *pending* state. Scan jobs run serially, in the order that they are started.

As the Discovery server reaches a specific scan job in the queue, that scan job transitions from the *pending* state to the *running* state as the processing of that scan job begins. If the scan process completes successfully, the scan job transitions to the *completed* state and the scan job produces results that can be viewed in a report. If the scan process results in an error that prevents successful completion of the scan, the scan job halts and the scan job transitions to the *failed* state. An additional status message for the failed scan contains information to help determine the cause of the failure.

Other states for a scan job result from user action that is taken on the scan job. You can pause or cancel a scan job while it is pending or running. A scan job in the *paused* state can be resumed. A scan job in the *canceled* state cannot be resumed.

CHAPTER 5. DOWNLOADING REPORTS

After you run a scan, you can download the reports for that scan to view the data that was gathered and processed during that scan.

Learn more

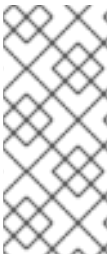
To learn more about downloading reports, see the following information:

- Downloading reports

5.1. DOWNLOADING REPORTS

After you run a scan, you can download the reports for that scan to view the data that was gathered and processed during that scan.

Reports for a scan are available in two formats, a comma-separated variable (CSV) format and a JavaScript Object Notation (JSON) format. They are also available in two content types, raw output from the scan as a details report and processed content as a deployments report.



NOTE

A third type of report is available, the insights report, but this report can be generated only through the Discovery command line interface. Downloading the insights report provides a **.tar.gz** file that you can transfer to the Hybrid Cloud Console at cloud.redhat.com. Transferring this file allows the report data to be used in the Red Hat Insights inventory service and in the subscriptions service.

Learn more

To learn more about merging and downloading reports, see the following information:

- Downloading reports

To learn more about how reports are created, see the following information. This information includes a chronology of the processes of report generation. These processes change the raw facts of a details report into fingerprint data, and then change fingerprint data into the deduplicated and merged data of a deployments report. This information also includes a partial fingerprint example to show the types of data that are used to create a Discovery report.

- How reports are created
- A fingerprint example

5.1.1. Downloading reports

From the Scans view, you can select one or more reports and download them to view the report data.

Prerequisites

If you want to download a report for a scan, the most recent scan job for that scan must have completed successfully.

Procedure

1. From the Scans view, navigate to the row of the scan for which you want to download the report.
2. Click **Download** for that scan.

Verification steps

The downloaded report is saved to the downloads location for your browser as a **.tar.gz** file, for example, **report_id_224_20190702_173309.tar.gz**. The filename format is **report_id_*ID*_*DATE*_*TIME*.tar.gz**, where ***ID*** is the unique report ID assigned by the server, ***DATE*** is the date in *yyyymmdd* format, and ***TIME*** is the time in the *hhmmss* format, based on the 24-hour system. The date and time data is determined by the interaction of the browser that is running the client with the server APIs.

To view the report, uncompress the **.tar.gz** file into a **report_id_*ID*** directory. The uncompressed report bundle includes four report files: two details reports in CSV and JSON formats, and two deployments reports in CSV and JSON formats.

NOTE

While you can view and use the output of these reports for your own internal processes, the Discovery documentation does not provide any information to help you interpret report results. In addition, although Red Hat Support can provide some basic assistance related to the installation and use of Discovery, the support team does not provide any assistance to help you understand the reports. The reports and their format are designed to be used by the Red Hat Subscription Education and Awareness Program (SEAP) team during customer engagements and for other Red Hat internal processes, such as providing data to various Hybrid Cloud Console services.

5.1.2. How reports are created

The scan process is used to discover the systems in your IT infrastructure, to inspect and gather information about the nature and contents of those systems, and to create a report from the information that it gathers during the inspection of each system.

A *system* is any entity that can be interrogated by the inspection tasks through an SSH connection, vCenter Server data, the Satellite Server API, or the Red Hat OpenShift cluster API. Therefore, a system can be a machine, such as a physical or virtual machine, and it can also be a different type of entity, such as a container or a cluster.

5.1.2.1. Facts and fingerprints

During a scan, a collection of facts is gathered for each system that is contained in each source. A *fact* is a single piece of data about a system, such as the version of the operating system, the number of CPU cores, or a consumed entitlement for a Red Hat product.

Facts are processed to create a summarized set of data for each system, data that is known as a fingerprint. A *fingerprint* is the set of facts that identifies a unique system and its characteristics, including the architecture, operating system, the different products that are installed on that system and their versions, the entitlements that are in use on that system, and so on.

Fingerprinting data is generated when you run a scan job, but the data is used to create only one type of report. When you request a details report, you receive the raw facts for that scan without any fingerprinting. When you request a deployments report, you receive the fingerprinting data that includes the results from the deduplication, merging, and post-processing processes. These processes include identifying installed products and versions from the raw facts, finding consumed entitlements, finding and merging duplicate instances of products from different sources, and finding products installed in nondefault locations, among other steps.

5.1.2.2. System deduplication and system merging

A single system can be found in multiple sources during a scan. For example, a virtual machine on vCenter Server could be running a Red Hat Enterprise Linux operating system installation that is also managed by Satellite. If you construct a scan that contains each type of source, vcenter, satellite, and network, that single system is reported by all three sources during the scan.

NOTE

Currently, you cannot combine an OpenShift or Ansible source with any other type of source in a scan, so deduplication and merging processes do not apply for an OpenShift or Ansible scan.

To resolve this issue and build an accurate fingerprint, Discovery feeds unprocessed system facts from the scan into a fingerprint engine. The fingerprint engine matches and merges data for systems that are found in more than one source by using the deduplication and merge processes.

The system deduplication process uses specific facts about a system to identify duplicate systems. The process moves through several phases, using these facts to combine duplicate systems in successively broader sets of data:

- All systems from network sources are combined into a single network system set. Systems are considered to be duplicates if they have the same value for the **subscription_manager_id** or **bios_uuid** facts.
- All systems from vcenter sources are combined into a single vcenter system set. Systems are considered to be duplicates if they have the same value for the **vm_uuid** fact.
- All systems from satellite sources are combined into a single satellite system set. Systems are considered to be duplicates if they have the same value for the **subscription_manager_id** fact.
- The network system set is merged with the satellite system set to form a single network-satellite system set. Systems are considered to be duplicates if they have the same value for the **subscription_manager** fact or matching MAC address values in the **mac_addresses** fact.
- The network-satellite system set is merged with the vcenter system set to form the complete system set. Systems are considered to be duplicates if they have matching MAC address values in the **mac_addresses** fact or if the vcenter value for the **vm_uuid** fact matches the network value for the **bios_uuid** fact.

5.1.2.2.1. System merging

After the deduplication process determines that two systems are duplicates, the next step is to perform a merge of those two systems. The merged system has a union of system facts from each source. When a fact that appears in two systems is merged, the merge process uses the following order of precedence to merge that fact, from highest to lowest:

1. network source fact
2. satellite source fact
3. vcenter source fact

A system fingerprint contains a **metadata** dictionary that captures the original source of each fact for that system.

5.1.2.3. System post-processing

After deduplication and merging are complete, there is a post-processing phase that creates derived system facts. A *derived system fact* is a fact that is generated from the evaluation of more than one system fact. The majority of derived system facts are related to product identification data, such as the presence of a specific product and its version.

The following example shows how the derived system fact **system_creation_date** is created.

The **system_creation_date** fact is a derived system fact that contains the real system creation time. The value for this fact is determined by the evaluation of the following facts. The value for each fact is examined in the following order of precedence, with the order of precedence determined by the accuracy of the match to the real system creation time. The highest non-empty value is used to determine the value of the **system_creation_date** fact.

1. **date_machine_id**
2. **registration_time**
3. **date_anaconda_log**
4. **date_filesystem_create**
5. **date_yum_history**

5.1.2.4. Report creation

After the processing of the report data is complete, the report creation process builds two reports in two different formats, JavaScript Object Notation (JSON) and comma-separated variable (CSV). The *details* report for each format contains the raw facts with no processing, and the *deployments* report for each format contains the output after the raw facts have passed through the fingerprinting, deduplication, merge, and post-processing processes.

The report format is designed to be used by the Red Hat Subscription Education and Awareness Program (SEAP) team during customer engagements and for other Red Hat internal processes.

NOTE

While you can view and use the output of these reports for your own internal processes, the Discovery documentation does not provide any information to help you interpret report results. In addition, although Red Hat Support can provide some basic assistance related to the installation and use of Discovery, the support team does not provide any assistance to help you understand the reports. The reports and their format are designed to be used by the Red Hat Subscription Education and Awareness Program (SEAP) team during customer engagements and for other Red Hat internal processes, such as providing data to various Hybrid Cloud Console services.

5.1.2.5. A fingerprint example

A fingerprint is composed of a set of facts about a single system in addition to facts about products, entitlements, sources, and metadata on that system. The following example shows fingerprint data. A fingerprint for a single system, even with very few Red Hat products installed on it, can be many lines. Therefore, only a partial fingerprint is used in this example.

Example

```
{
    "os_release": "Red Hat Enterprise Linux Atomic Host 7.4",
    "cpu_count": 4,
    "products": [
        {
            "name": "JBoss EAP",
            "version": null,
            "presence": "absent",
            "metadata": {
                "source_id": 5,
                "source_name": "S62Source",
                "source_type": "satellite",
                "raw_fact_key": null
            }
        }
    ],
    "entitlements": [
        {
            "name": "Satellite Tools 6.3",
            "entitlement_id": 54,
            "metadata": {
                "source_id": 5,
                "source_name": "S62Source",
                "source_type": "satellite",
                "raw_fact_key": "entitlements"
            }
        }
    ],
    "metadata": {
        "os_release": {
            "source_id": 5,
            "source_name": "S62Source",
            "source_type": "satellite",
            "raw_fact_key": "os_release"
        },
        "cpu_count": {
            "source_id": 4,
            "source_name": "NetworkSource",
            "source_type": "network",
            "raw_fact_key": "os_release"
        }
    },
    "sources": [
        {
            "id": 4,
            "source_type": "network",
            "name": "NetworkSource"
        },
        {
            "id": 5,
            "source_type": "satellite",
            "name": "S62Source"
        }
    ]
}
```

The first several lines of a fingerprint show facts about the system, including facts about the operating system and CPUs. In this example, the **os_release** fact describes the installed operating system and release as **Red Hat Enterprise Linux Atomic Host 7.4**.

Next, the fingerprint lists the installed products in the **products** section. A product has a name, version, presence, and metadata field. In the JBoss EAP section, the **presence** field shows **absent** as the value, so the system in this example does not have Red Hat JBoss Enterprise Application Platform installed.

The fingerprint also lists the consumed entitlements for that system in the **entitlements** section. Each entitlement in the list has a name, ID, and metadata that describes the original source of that fact. In the example fingerprint, the system has the **Satellite Tools 6.3** entitlement.

In addition to the metadata fields that are in the **products** and **entitlements** sections, the fingerprint contains a **metadata** section that is used for system fact metadata. For each system fact, there is a corresponding entry in the **metadata** section of the fingerprint that identifies the original source of that system fact. In the example, the **os_release** fact was found in Satellite Server, during the scan of the satellite source.

Lastly, the fingerprint lists the sources that contain this system in the **sources** section. A system can be contained in more than one source. For example, for a scan that includes both a network source and a satellite source, a single system can be found in both parts of the scan.

CHAPTER 6. SENDING REPORTS TO THE HYBRID CLOUD CONSOLE

After you run a scan, you can send reports for that scan to the Hybrid Cloud Console at cloud.redhat.com. The report that you generate and send is not a details report or a deployments report. Instead, it is a third type of report known as an *insights report*. This type of report is formatted especially for ingestion by the Hybrid Cloud Console services.

When you send insights reports to the Hybrid Cloud Console, the report data can be ingested and used by Hybrid Cloud Console services, such as the inventory service of Red Hat Insights to display host-based inventory data and the subscriptions service to display subscription usage data.

Learn more

To learn more about how to work with insights reports, see the following information:

- Downloading and sending insights reports to the Hybrid Cloud Console

To learn more about insights reports concepts, see the following information:

- What is an insights report?

6.1. DOWNLOADING AND SENDING INSIGHTS REPORTS TO THE HYBRID CLOUD CONSOLE

When you need to provide report data to the Hybrid Cloud Console services such as the Red Hat Insights inventory service and the subscriptions service, you download and send an insights report.

This type of report is different from a details report or a deployments report. An *insights report* is a Discovery report with data that is similar to the deployments report, but its contents and format are designed especially to be ingested and used by the Hybrid Cloud Console services. In addition, the insights report cannot be created from the Discovery graphical user interface. It must be created by using the Discovery command line interface.

Prerequisites

If you want to download and send an insights report, you must meet the following requirements:

- The most recent scan job for that scan must have completed successfully.
- The Discovery command line interface must be installed on the same system as the Discovery server so that you can run the following procedure from the command line interface. You cannot download and send an insights report from the graphical user interface.

Procedure

1. Log in to the command line interface, where ***server_administrator_username*** is the username for the Discovery server administrator and ***server_administrator_password*** is the password for the server administrator:

   ```
   $ dsc server login --username server_administrator_username --password
   server_administrator_password
   ```

2. Find the **report_identifier** (report ID) value for the scan job that you want to use to create an insights report. The following command returns the summary details for all created scan objects:

```
$ dsc scan list
```

NOTE

If you know the name of the scan that you want to use, but do not know the **report_identifier** value, you can also use the **qpc scan show --name *scan_name*** command to show the scan jobs for that scan only.

3. Using the **report_identifier** value that you located, download the insights report for the scan job. In the following example command, the file name assigned to the downloaded report is **report.tar.gz** but you can change this filename as needed:

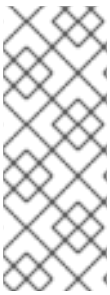
```
$ dsc report insights --report report_identifier --output-file report.tar.gz
```

4. Add the credentials that you use to log in to the Hybrid Cloud Console, generally your Red Hat Customer Portal account, to the command line interface configuration. This step is needed so that these credentials can be used in the next step to send the insights report to the Hybrid Cloud Console.

```
$ dsc insights login --username hcc_username --password
```

5. Use the **publish** subcommand to send the insights report data to the Hybrid Cloud Console and the services that can consume the reports, such as the inventory service and the subscriptions service.

```
$ dsc insights publish --input-file report.tar.gz
```



NOTE

While you can view the output of insights reports, the Discovery documentation does not provide any information to help you interpret insights report results. In addition, although Red Hat Support can provide some basic assistance related to the installation and use of Discovery, the support team does not provide any assistance to help you understand the insights reports. The insights reports and their format are designed to be used by Red Hat internal processes, such as providing data to various Hybrid Cloud Console services.

Additional resources

- For more information about installing and configuring the Discovery command line interface, see the *Installing and configuring Discovery* guide.

6.2. WHAT IS AN INSIGHTS REPORT?

After you run a scan on your IT infrastructure or parts of your IT infrastructure, you can use Discovery to create an insights report with the data from the scan. The insights report is a specialized report that is intended to be sent to Hybrid Cloud Console services, such as the inventory service of Red Hat Insights to display host-based inventory data and the subscriptions service to display subscription usage data.

Although Discovery is useful for scanning and reporting on all parts of your IT infrastructure, both connected and disconnected, the ability to send an insights report to the Hybrid Cloud Console services is particularly useful if parts of your IT infrastructure are disconnected, or air-gapped. By using Discovery to gather data about those parts of your network, you can get a more complete and more curated view

of your overall network. When the data from an insights report is combined with the other data collection from the tools that support the Hybrid Cloud Console, it enables you to see a unified inventory and a complete picture of subscription usage in a single place, the Hybrid Cloud Console.

6.2.1. Frequency of reporting

All disconnected or air-gapped systems must be periodically scanned and reported through an insights report to ensure that accurate data is reaching the Hybrid Cloud Console. A weekly cadence of sending an insights report is the current recommendation. A weekly cadence provides sufficient milestones for effectively monitoring subscription usage in the subscriptions service.

6.2.2. Avoiding system duplication

Depending on the type of data that you are providing in the insights report, the masking of data can interfere with the quality of that report, especially for the deduplication and merge processes of report creation.

For example, if the insights report contains data for both connected and disconnected parts of your IT infrastructure, and you are masking data in that report, connected systems that are also being reported through other methods such as Red Hat Satellite or Red Hat Insights will be duplicated. Therefore, if you already have systems that are being reported directly through Red Hat Insights, Satellite, Red Hat Subscription Management, or similar tools, you should avoid masking hostnames, IP addresses, and similar facts that help differentiate systems when you generate an insights report.

In general, for scans that cover only disconnected parts of your IT infrastructure, or scans for 100% disconnected customers, masking is an optional step if consistent hash values are used. However, masking is not recommended. Because masking eliminates the type of information that is used to help distinguish individual systems, the use of masking prevents you from gaining the majority of benefits that are provided by Red Hat Insights and other Hybrid Cloud Console tools such as the subscriptions service.