Subscription Central 1-latest

Troubleshooting Discovery

Troubleshooting Discovery

Last Updated: 2024-06-25

Subscription Central 1-latest Troubleshooting Discovery

Troubleshooting Discovery

Legal Notice

Abstract

Table of Contents

CHAPTER 1. ABOUT DISCOVERY 3
1.1. WHAT IS DISCOVERY? 3
1.2. WHAT PRODUCTS DOES DISCOVERY FIND? 4
1.3. IS DISCOVERY RIGHT FOR ME? 5

CHAPTER 2. TROUBLESHOOTING DISCOVERY 6
2.1. DETERMINING THE VERSION OF THE DISCOVERY SERVER 6
2.2. UNINSTALLING DISCOVERY 6
2.3. GETTING HELP WITH THE COMMAND LINE INTERFACE 7
2.4. UNABLE TO RUN DSC COMMANDS WITH THE COMMAND LINE INTERFACE 7
2.5. SSH CREDENTIAL CONFIGURATION 7
2.6. LOG FILE LOCATIONS 8
2.7. UNABLE TO CONNECT TO THE DISCOVERY SERVER WITH THE COMMAND LINE INTERFACE 8
2.8. BACKING UP OR RESTORING THE DISCOVERY DATABASE 9
2.9. BACKING UP OR RESTORING SSH CREDENTIALS 9
2.10. BACKING UP OR RESTORING ENCRYPTED SSH CREDENTIALS 9
2.11. RESTARTING THE DISCOVERY SERVER AFTER A REBOOT 10

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:

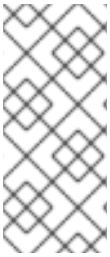
- Is Discovery right for me?

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. TROUBLESHOOTING DISCOVERY

2.1. DETERMINING THE VERSION OF THE DISCOVERY SERVER

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.
- You will need sudo access to perform certain functions in Podman.

Procedure

To determine the version of the Discovery server, use the following steps:

- Enter the **dsc server status** command. The expected output provides the version of the server that you are using:

```
"server_address": "127.0.0.1:9443", "server_id":
"45a8ea20-2ec4-4113-b459-234fed505b0d", "server_version":
"1.0.0.3e15fa8786a974c9eafe6376ff31ae0211972c36"
```

  If you cannot get the server status command to run, or you cannot log in to the server, use the following Podman images command:

```
podman images --filter 'reference=registry.redhat.io/discovery/discovery-server-rhel9:latest' --
format '{{.Labels.url}}'
```

2.2. UNINSTALLING DISCOVERY

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.
- You will need sudo access to perform certain functions in Podman.

Procedure

To uninstall Discovery servers, use the following steps:

1. Stop the containers and remove the pod.

```
$ podman stop discovery
$ podman stop dsc-db
$ podman pod rm discovery-pod
```

2. Remove the Discovery container images.

```
$ podman rmi registry.redhat.io/discovery/discovery-server-rhel9

$ podman rmi registry.redhat.io/rhel9/postgresql-15
```

3. Remove the storage volumes.

```
$ podman volume rm dsc-data
```

4. Uninstall the command line interface, if installed.

```
$ sudo dnf remove dsc
```

2.3. GETTING HELP WITH THE COMMAND LINE INTERFACE

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.

Procedure

- For help on general topics, see the man page information.
- For help on a specific subcommand, use the **-h** option. For example:

```
$ dsc cred -h
$ dsc source -h
$ dsc scan -h
```

2.4. UNABLE TO RUN DSC COMMANDS WITH THE COMMAND LINE INTERFACE

The following error message or a similar message might indicate that you have not established the **dsc** alias command for Discovery.

bash: dsc: command not found

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.
- You will need sudo access to perform certain functions in Podman.

Procedure

To create the **dsc** alias, use the following commands:

```
$ podman exec dsc-db psql -c 'CREATE ROLE dsc LOGIN PASSWORD' <username>
$ podman exec dsc-db psql -c 'GRANT ALL PRIVILEGES ON DATABASE' "dsc-db" to dsc
```

Verification

If the second command fails, the database may not exist. To create the database, use the following command:

```
$ podman exec dsb-db psql -c 'CREATE DATABASE "dsc-db"'
```

2.5. SSH CREDENTIAL CONFIGURATION

If you receive an error message that includes text similar to **not a valid file on the filesystem**, that message might indicate an issue with the mount point on the file system that enables access to the SSH keyfiles.

When you are creating your network credentials with SSH keyfiles, make sure that the copy of the private key has been correctly added to the **"${HOME}"/.local/share/discovery/sshkeys** directory on the server.

Detailed information about credential configuration and authentication with SSH keyfiles is available in Adding SSH keys to the discovery server for network scans .

2.6. LOG FILE LOCATIONS

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.

Procedure

Log files for the Discovery server that are on the local file system are located in the following path: **"{HOME}"/.local/share/discovery/log**.

Log files for the container itself can be accessed with the following command:

```
$ podman exec -it discovery bash
$ cd "{HOME}"/.local/share/discovery/log/
```

Log data is also copied to **stdout** and can be accessed through Podman logs. To follow the log output, include the **-f** option as shown in the following command:

```
$ podman logs -f discovery
```

2.7. UNABLE TO CONNECT TO THE DISCOVERY SERVER WITH THE COMMAND LINE INTERFACE

The following error message or a similar message might indicate an issue with the Discovery server:

A connection error occurred while attempting to communicate with the server

Restore the server by restarting the server pod.

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.
- You will need sudo access to perform certain functions in Podman.

Procedure

To restore the Discovery server, use the following command:

```
$ podman pod start discovery-pod
```

2.8. BACKING UP OR RESTORING THE DISCOVERY DATABASE

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.
- You might need sudo access to perform certain functions in Podman.

Procedure

- To back up the Discovery database, use the **pg_dump** command to create a script dump of the data. When prompted, enter the credentials for the Discovery database administrator.
- To restore a previous database to a new or upgraded Discovery server, use the following commands, where ***dump.sql*** is the example name of the script dump file:

```
$ podman cp _dump.sql_ dsc-db:.
$ podman exec dsc-db psql -f _dump.sql_
$ podman exec dsc-db rm _dump.sql_
```

2.9. BACKING UP OR RESTORING SSH CREDENTIALS

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.

Procedure

- To back up the SSH credentials, navigate to the following directory and copy the SSH keyfile directory: **"${HOME}"/.local/share/discovery/sshkeys**
- To restore the SSH credentials, use the following command, where *SSHkeys_backup_directory* is the path of the SSH keyfile backup directory where the individual keyfiles are backed up:

```
$ cp -p __SSHkeys_backup_directory__/* "${HOME}"/.local/share/discovery/sshkeys/
```

2.10. BACKING UP OR RESTORING ENCRYPTED SSH CREDENTIALS

Passwords are not stored as plain text. They are encrypted and decrypted by using the content of the **secret.txt** file as a secret key. If you need to back up and restore the **secret.txt** file, use these steps.

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.

Procedure

- To back up the encrypted SSH credentials, navigate to **"${HOME}"/.local/share/discovery/data** directory and copy the **secret.txt** file.
- To restore the **secret.txt** file, enter the following command, where *path_to_backup* is the path where the **secret.txt** file is backed up:

```
$ cp -p __path_to_backup__/secret.txt "${HOME}"/.local/share/discovery/data/
```

2.11. RESTARTING THE DISCOVERY SERVER AFTER A REBOOT

Prerequisites

- You must be logged in to the command line interface as the Discovery server administrator.
- You will need sudo access to perform certain functions in Podman.

Procedure

- To restart the Discovery server after a reboot, use the following command:

```
$ podman pod restart discovery-pod
```