Subscription Central 2023

Discovery のトラブルシューティング

Discovery のトラブルシューティング

Last Updated: 2023-11-15

Subscription Central 2023 Discovery のトラブルシューティング

Discovery のトラブルシューティング

法律上の通知

概要

目次

第1章 DISCOVERY について

製品検出ツールは、特定の Red Hat ソフトウェアの使用状況に関するデータをユーザーが収集できるように設計されています。Discovery を使用すると、Red Hat 製品の使用状況を計算して報告するのに必要な時間と作業量を減らすことができます。

詳細情報

Discovery の目的、利点、および特長の詳細は、以下の情報を参照してください。

- Discovery とは

Discovery が検出および検査可能な製品および製品バージョンの詳細は、以下の情報を参照してください。

- Discovery が検出する製品

Discovery が適切なソリューションであるかどうかを評価するには、以下の情報を参照してください。

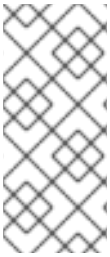
- Discovery が適切かどうか

1.1. DISCOVERY とは

Discovery とも呼ばれる製品検出ツールは、検査およびレポートツールです。これは、ネットワーク上の物理システムと仮想システムの数、そのシステムのオペレーティングシステム、その他の設定データなどの環境データまたはファクトを検出、識別、および報告するように設計されています。さらに、ネットワーク内の IT リソースの主要な Red Hat パッケージおよび製品の一部のバージョンについて、より詳細なファクトを見つけ、特定し、報告するように設計されています。

ネットワーク上で実行されているソフトウェアとシステムを検査できるため、サブスクリプションの使用状況を理解し、報告する能力が向上します。最終的には、このような検査と報告のプロセスは、インベントリー管理という、より大きなシステム管理タスクの一部です。

製品検出ツールは、IT リソースにアクセスし、検査プロセスを実行するために、2 つの基本的な構造の設定を必要とします。**認証情報** には、特定のソースまたはそのソースの一部のアセットで検査プロセスを実行するのに十分な権限を持つユーザーのユーザー名、パスワードまたは SSH キーなどのユーザーアクセスデータが含まれています。**ソース** には、検証される単一または複数のアセットに関するデータが含まれています。これらのアセットは、ホスト名、IP アドレス、IP 範囲、またはサブネットとして識別される物理マシン、仮想マシン、またはコンテナーです。また、これらのアセットは、vCenter Server や Red Hat Satellite Server などのシステム管理ソリューションや、Red Hat OpenShift Container Platform にデプロイされたクラスターである場合もあります。



注記

現在、仮想化インフラストラクチャー専用のソースを使用して Discovery でスキャンできる唯一の仮想化されたデプロイメントは、VMware vCenter です。Red Hat がサポートする他の仮想化インフラストラクチャーは、専用のスキャンでは検出できません。ネットワークの一般的なスキャンでは、専用のスキャンで正確なメタデータが返されない場合も、これらのアセットが検出される場合があります。

複数の認証情報およびソースを保存しておき、検査プロセスまたは **スキャン** の実行時にさまざまに組み合わせて Discovery で使用できます。スキャンが完了したら、フォーマットされたデータのコレクションや **レポート** の形式で出力に含まれるこれらのファクトにアクセスして、結果を確認できます。

デフォルトでは、Discovery の使用中に作成された認証情報およびソースはデータベースで暗号化され

ます。値は AES-256 暗号化で暗号化されます。これらの認証情報およびソースは、Discovery サーバーが Vault パスワードを使用してスキャンを実行し、データベースに保存されている暗号化された値にアクセスする際に復号化されます。

製品検出ツールはエージェントレス検査ツールであるため、検査されるすべてのソースにツールをインストールする必要はありません。ただし、Discovery がインストールされているシステムは、検出および検証されるシステムにアクセスできる必要があります。

1.2. DISCOVERY が検出する製品

製品検出ツールは、以下の Red Hat 製品を検出します。各バージョンまたはリリースについて、最も古いバージョンを記載し、それ以降のリリースを検出対象として示しています。

製品の現在の名前をより理解しやすくするために、製品の名前が最近変更になっている場合は、その名前を追加情報として提供しています。新しい製品名が記載されていても、その製品の特定のバージョンが併せて記載されていない限り、それ以降のバージョンは対象外です。

Red Hat Enterprise Linux

- Red Hat Enterprise Linux バージョン 5 以降
- Red Hat Enterprise Linux バージョン 6 以降
- Red Hat Enterprise Linux バージョン 7 以降
- Red Hat Enterprise Linux バージョン 8 以降
- Red Hat Enterprise Linux バージョン 9 以降

Red Hat Application Services 製品 (旧称 Red Hat Middleware)

- Red Hat JBoss BRMS バージョン 5.0.1 以降、バージョン 6.0.0 以降 (Red Hat Decision Manager とも呼ばれ、現在は Red Hat Process Automation Manager の一部)
- JBoss Enterprise Web Server バージョン 1 以降、Red Hat JBoss Web Server 3.0.1 以降
- Red Hat JBoss Enterprise Application Platform バージョン 4.2 以降、バージョン 4.3 以降、バージョン 5 以降、バージョン 6 以降、バージョン 7 以降
- Red Hat Fuse バージョン 6.0 以降

Red Hat Ansible Automation Platform

- Ansible Automation Platform バージョン 2 以降

Red Hat OpenShift Container Platform

- Red Hat OpenShift Container Platform バージョン 4 以降

Kubernetes 用 Red Hat Advanced Cluster Security

- Red Hat Advanced Cluster Security for Kubernetes バージョン 4 以降

Red Hat Advanced Cluster Management for Kubernetes

- Red Hat Advanced Cluster Management for Kubernetes バージョン 2 以降

1.3. DISCOVERY が適切かどうか

製品検出ツールは、複雑なネットワーク全体における未知の製品の使用状況を含め、Red Hat 製品のインベントリーの検出および理解を支援することを目的としたものです。Discovery によって生成されたレポートは、Red Hat ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) とのパートナーシップや、Subscription Education and Awareness Program (SEAP) が提供する分析と支援を活用することで、理解が容易になります。

個別に Discovery をインストールして使用し、レポートデータを生成して表示できますが、Discovery ドキュメントではレポート結果の解釈に役立つ情報は提供していません。さらに、Red Hat サポートは Discovery のインストールおよび使用方法に関する基本的なサポートは提供しますが、レポートを理解するためのサポートは提供しません。

Discovery ツールは、Red Hat と直接データを自動的に共有しません。代わりに、Red Hat のツールとサービスに取り込むために、レポートデータを準備して Red Hat に送信するかどうかを選択できます。Discovery ツールをローカルで使用してネットワークをスキャンし、Discovery が現在サポートしている Red Hat 製品を検出して、生成されたレポートを内部目的で使用できます。

第2章 DISCOVERY のトラブルシューティング

2.1. DISCOVERY サーバーのバージョンの判別

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。
- Podman で特定の機能を実行する場合、sudo アクセス権を持っている。

手順

Discovery サーバーのバージョンを確認するには、以下の手順に従います。

- **dsc server status** コマンドを入力します。予想される出力に、使用しているサーバーのバージョンが提示されます。

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

server status コマンドを実行できない場合、またはサーバーにログインできない場合は、次の podman images コマンドを使用します。

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

2.2. DISCOVERY のアンインストール

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。
- Podman で特定の機能を実行する場合、sudo アクセス権を持っている。

手順

Discovery サーバーをアンインストールするには、以下の手順に従います。

1. コンテナーを停止し、Pod を削除します。

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

2. Discovery コンテナーイメージを削除します。

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

$ podman rmi registry.redhat.io/rhel9/postgresql-12
```

3. ストレージボリュームを削除します。

```
$ podman volume rm dsc-db
```

4. コマンドラインインターフェイスがインストールされている場合は、アンインストールします。

```
$ sudo dnf remove dsc
```

2.3. コマンドラインインターフェイスでのヘルプの取得

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。

手順

- 一般的なトピックに関するヘルプは、man ページの情報を参照してください。

注記

現在、Discovery コマンドラインインターフェイスから man ページ情報は利用できません。man ページ情報には、製品検出ツールのアップストリームプロジェクトである **quipucords** リポジトリーでアクセスできます。man ページ情報は、このプロジェクトの **qpc** サブリポジトリーにあります。

Discovery コマンドの使用方法は、https://github.com/quipucords/qpc/blob/master/docs/source/man.rst の qpc man ページを参照してください。コマンドラインインターフェイスの使用を開始する場合は、コマンドラインエントリーの **qpc** コマンドを **dsc** コマンドに置き換えます。

- 特定のサブコマンドのヘルプを表示するには、**-h** オプションを使用します。以下に例を示します。

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

2.4. コマンドラインインターフェイスで DSC コマンドを実行できない場合

次のエラーメッセージまたは同様のメッセージは、Discovery 用の **dsc** エイリアスコマンドが確立されていないことを示している可能性があります。

bash: dsc: command not found

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。
- Podman で特定の機能を実行する場合、sudo アクセス権を持っている。

手順

dsc エイリアスを作成するには、次のコマンドを使用します。

```
$ 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
```

検証

2 番目のコマンドが失敗した場合は、データベースが存在しない可能性があります。データベースを作成するには、次のコマンドを使用します。

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

2.5. SSH 認証情報の設定

not a valid file on the filesystem のようなテキストを含むエラーメッセージが表示された場合、そのメッセージは、SSH キーファイルにアクセスできるようにするファイルシステムのマウントポイントに問題があることを示している可能性があります。

SSH キーファイルを使用してネットワーク認証情報を作成する場合は、秘密鍵のコピーがサーバーの **"${HOME}"/.local/share/discovery/sshkeys** ディレクトリーに正しく追加されていることを確認します。

SSH キーファイルを使用した認証情報の設定および認証の詳細は、ネットワークスキャン用の Discovery サーバーに SSH キーを追加 を参照してください。

2.6. ログファイルの場所

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。

手順

ローカルファイルシステムにある Discovery サーバーのログファイルは、**{HOME}"/.local/share/discovery/log** にあります。

コンテナー自体のログファイルには、以下のコマンドを使用してアクセスできます。

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

ログデータは **stdout** にコピーされ、Podman ログからアクセスできます。ログ出力を追跡するには、以下のコマンドに示すように **-f** オプションを追加します。

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

2.7. コマンドラインインターフェイスを使用して DISCOVERY サーバーに接続できない場合

次のエラーメッセージまたは同様のメッセージは、Discovery サーバーに問題があることを示している可能性があります。

A connection error occurred while attempting to communicate with the server

サーバー Pod を再起動して、サーバーを復元します。

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。
- Podman で特定の機能を実行する場合、sudo アクセス権を持っている。

手順

Discovery サーバーを復元するには、次のコマンドを使用します。

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

2.8. DISCOVERY データベースのバックアップまたは復元

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。
- Podman で特定の機能を実行する場合、sudo アクセス権を持っている。

手順

- Discovery データベースをバックアップするには、**pg_dump** コマンドを使用してデータのスクリプトダンプを作成します。プロンプトが表示されたら、Discovery データベース管理者の認証情報を入力します。
- 以前のデータベースを新規またはアップグレードされた Discovery サーバーに復元するには、以下のコマンドを使用します。**dump.sql** は、スクリプトダンプファイルの例です。

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

2.9. SSH 認証情報のバックアップまたは復元

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。

手順

- SSH 認証情報をバックアップするには、**"${HOME}"/.local/share/discovery/sshkeys** ディレクトリーに移動し、SSH キーファイルディレクトリーをコピーします。
- SSH 認証情報を復元するには、以下のコマンドを使用します。**SSHkeys_backup_directory** は、個々のキーファイルがバックアップされる SSH キーファイルバックアップディレクトリーのパスです。

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

2.10. 暗号化された SSH 認証情報のバックアップまたは復元

パスワードはプレインテキストとして保存されません。これらは、**secret.txt** ファイルの内容を秘密鍵として使用し、暗号化および復号化されます。**secret.txt** ファイルをバックアップして復元する必要がある場合は、以下の手順に従います。

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。

手順

- 暗号化された SSH 認証情報をバックアップするには、**"${HOME}"/.local/share/discovery/data** ディレクトリーに移動し、**secret.txt** ファイルをコピーします。
- **secret.txt** ファイルを復元するには、以下のコマンドを入力します。**path_to_backup** は、**secret.txt** ファイルがバックアップされるパスです。

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

2.11. 再起動後の DISCOVERY サーバーの再起動

前提条件

- Discovery サーバー管理者としてコマンドラインインターフェイスにログインしている。
- Podman で特定の機能を実行する場合、sudo アクセス権を持っている。

手順

- 再起動後に Discovery サーバーを再起動するには、以下のコマンドを使用します。

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