



Red Hat Subscription Management 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

Red Hat Subscription Management 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

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

目次

第1章 DISCOVERY について	3
1.1. DISCOVERY とは	3
1.2. DISCOVERY が検出する製品	4
1.3. DISCOVERY が適切かどうか	4
第2章 DISCOVERY のトラブルシューティング	6
2.1. DISCOVERY サーバーのバージョンの判別	6
2.2. DISCOVERY のアンインストール	6
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	7
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	7
2.5. SSH 認証情報の設定	8
2.6. ログファイルの場所	8
2.7. コマンドラインインターフェイスを使用して検出サーバーに接続できない場合	8
2.8. DISCOVERY データベースのバックアップと復元	9
2.9. SSH 認証情報のバックアップと復元	9
2.10. 暗号化された SSH 認証情報のバックアップと復元	9
2.11. 再起動後の DISCOVERY サーバーの再起動	10

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中のソフトウェアおよびシステムを検査する機能は、サブスクリプションの使用状況を把握して報告する機能を強化します。最終的に、この検査およびレポートプロセスは、インベントリを管理する大規模なシステム管理タスクの一部となります。

プロダクト検出ツールでは、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つの基本的な構造を設定する必要があります。**認証情報** 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ための十分な権限を持つユーザーのユーザー名とパスワードまたは 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、検証される単一のアセットまたは複数のアセットに関するデータが含まれます。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、特殊なスキャンで検出できません。ネットワークの一般的なスキャンでは、特殊なスキャンによって正確なメタデータが返されなくても、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、検査プロセスまたは **スキャン** の実行時にさまざまな組み合わせで Discovery と使用することができます。スキャンが完了したら、フォーマットされたデータ、または **report** のコレクションとして出力にあるこれらのファクトにアクセスし、結果を確認することができます。

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。Discovery サーバーは、Vault パスワードを使用してスキャンを実行して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 製品を見つけます。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が一覧表示され、後続のリリースは該当と示されています。

製品の名前が最近変更されており、その製品の現在の名前をよく理解している場合は、その名前が追加情報として提供されます。また、製品の特定のバージョンも記載されない限り、新しいバージョンの製品名が含まれることはありません。

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 ミドルウェア)

- 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 OpenShift Container Platform

- Red Hat OpenShift Container Platform バージョン 4 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での未知の製品の使用状況など、Red Hat 製品のインベントリを見つけて理解するのに役立つことを目的としています。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を通じて、または Subscription Education and Awareness Program (SEAP) によって提供される分析と支援を活用することで最も理解できます。

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を提供しますが、サポートチームはお客様がレポートを理解できるようにサポートするわけではありません。

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 ツールおよびサービスによる取り込みのために、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します。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 製品を探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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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。予想される出力には、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"
```

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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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 コンテナイメージを削除します。

```
# podman rmi registry.redhat.io/discovery/discovery-server-rhel8  
# podman rmi registry.redhat.io/rhel8/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. インストールされている場合は、コマンドラインインターフェイスをアンインストールします。

```
# 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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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、検出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。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** リポジトリの man ページ情報にアクセスできます。man ページ情報は、そのプロジェクトの **qpc** サブリポジトリにあります。

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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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 に似た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 `~/discovery/server/volumes/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について、詳しくは [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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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、`/var/discovery/server/volumes/log` のパスにあります。

コンテナ自体のログファイルは、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 /var/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検出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、検出サーバーの問題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する。

- 以下の手順でコマンドを実行するための root 権限または同等の権限。

手順

検出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と復元

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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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립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検出サーバーに復元するには、以下のコマンドを使用します。ここでの **dump.sql** は、スク립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と復元

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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

手順

- SSH 認証情報をバックアップするには、次の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:**/var/discovery/server/volumes/sshkeys**
- 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。ここでの、**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__/* /var/discovery/server/volumes/sshkeys/
```

2.10. 暗号化された SSH 認証情報のバックアップと復元

パスワードはプレー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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

手順

- 暗号化された SSH 認証情報をバックアップするには、`/var/discovery/volumes/data` ディレクトリに移動し、**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。ここでの `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 /var/discovery/volumes/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する。
- 以下の手順でコマンドを実行するための root 権限または同等の権限。

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
```