Subscription Central 1-latest

Discovery の使用

Discovery の理解

Last Updated: 2024-03-30

Subscription Central 1-latest Discovery の使用

Discovery の理解

法律上の通知

概要

目次

第1章 DISCOVERY について

Discovery 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際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 とは何ですか?

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。

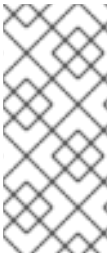
- Discovery が適切かどうか

1.1. DISCOVERY とは何ですか?

Discovery 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。

Discovery には、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。

Discovery はエージェントレスの検査ツールであるため、検査対象の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

Discovery は次の 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

Discovery は、複雑なネットワーク全体での不明な製品の使用状況など、Red Hat 製品インベントリーを検索して理解できるようにする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て、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 ユーザーインターフェイスへのアクセス

ブラウザー接続を使用して、Discovery グラフィカルユーザーインターフェイスにアクセスできます。

詳細情報

Discovery のグラフィカルユーザーインターフェイスへのログインおよびログアウトを行う要件および手順の詳細は、以下の情報を参照してください。

- Discovery ユーザーインターフェイスへのログイン
- Discovery ユーザーインターフェイスからログアウト

2.1. DISCOVERY ユーザーインターフェイスへのログイン

Discovery ユーザーインターフェイスにログインするには、Discovery サーバーがインストールされているシステムの IP アドレス、サーバーのインストール時にデフォルトのポートが変更された場合は接続のポート番号、ログイン時に使用する管理者ユーザーのユーザー名およびパスワードが必要です。この情報がない場合は、Discovery サーバーをインストールした管理者にお問い合わせください。

前提条件

- Discovery ユーザーインターフェイスを使用するために、グラフィカルユーザーインターフェイスを実行するシステムが、Discovery サーバーがインストールされているシステムと通信できるようになっている。

手順

1. ブラウザーで、Discovery サーバーの URL を **https://IPaddress:server_port** の形式で入力します。**IPaddress** は Discovery サーバーの IP アドレスで、 **server_port** は公開されたサーバーポートです。
   以下の例は、ログインしているシステムとデフォルトのポートを使用するかどうかに基づいて、URL を入力する 2 つの方法を示しています。

   - サーバーがインストールされ、デフォルトのポート **9443** が使用されるシステムからログインする場合は、以下の例のようにループバックアドレス (localhost とも呼ばれる) を IP アドレスとして使用できます。

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

   - サーバーからリモートになっているシステムからログインし、サーバーが IP アドレス **192.0.2.0** で稼働しており、インストール中にデフォルトのポートが **8443** に変更になった場合は、次の例のようにログインします。

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

   サーバーの URL を入力すると、Discovery ログインページが表示されます。

2. ログインページで、Discovery サーバー管理者アカウントのユーザー名とパスワードを入力し、**ログイン** をクリックしてサーバーにログインします。

検証手順

Discovery に初めてログインすると、Welcome ページが表示されます。まず、スキャンで使用できるソースおよび認証情報を追加します。Discovery に以前にログインしていると、Welcome ページはスキップされ、以前に作成したソース、認証情報、およびスキャンを操作できます。

2.2. DISCOVERY ユーザーインターフェイスからログアウト

手順

1. アプリケーションツールバーで、人のアイコンまたはユーザー名をクリックします。
2. **Logout** をクリックします。

第3章 ソースおよび認証情報の追加

スキャンを実行するために Discovery を準備するには、スキャンする IT インフラストラクチャーの一部を 1 つ以上のソースとして追加する必要があります。また、これらのソースへのアクセスに必要なユーザー名とパスワードや SSH キーなどの認証情報を 1 つ以上のクレデンシャルとして追加する必要があります。設定要件が異なるため、スキャンするソースのタイプに応じてソースと認証情報を追加します。

詳細情報

IT インフラストラクチャーのさまざまな部分を含むソースおよび認証情報を追加する一般的なプロセスの一部として、多数のタスクを完了する必要がある場合があります。

ネットワークソースおよび認証情報を追加して、ネットワーク上の物理マシン、仮想マシン、コンテナーなどのアセットをスキャンします。詳細は、以下の情報を参照してください。

- ネットワークソースおよび認証情報の追加

Satellite ソースと認証情報を追加して、Red Hat Satellite Server のデプロイメントをスキャンし、管理するアセットを見つけます。詳細は、以下の情報を参照してください。

- Satellite ソースおよび認証情報の追加

vCenter ソースおよび認証情報を追加して、vCenter Server のデプロイメントをスキャンし、管理するアセットを見つけます。詳細は、以下の情報を参照してください。

- vCenter ソースおよび認証情報の追加

OpenShift ソースおよび認証情報を追加して、Red Hat OpenShift Container Platform クラスターのデプロイメントをスキャンします。詳細は、以下の情報を参照してください。

- OpenShift ソースおよび認証情報の追加

Ansible ソースと認証情報を追加し、Ansible Automation Platform のデプロイメントをスキャンして、管理されているセキュアなクラスターを見つけます。詳細は、以下の情報を参照してください。

- Ansible ソースと認証情報の追加

RHACS ソースと認証情報を追加し、Red Hat Advanced Cluster Security for Kubernetes のデプロイメントをスキャンして、RHACS が管理するセキュアなクラスターを見つけます。詳細は、以下の情報を参照してください。

- RHACS ソースおよび認証情報の追加

3.1. ネットワークソースおよび認証情報の追加

ネットワーク上の 1 つ以上の物理マシン、仮想マシン、またはコンテナーでスキャンを実行するには、スキャンする各アセットを識別するソースを追加する必要があります。その後、各アセットにアクセスするために認証データが含まれる認証情報を追加する必要があります。

詳細情報

ネットワークソースと認証情報を 1 つ以上追加して、ネットワーク内のアセットをスキャンするのに必要な情報を提供します。詳細は、以下の情報を参照してください。

- ネットワークソースを追加するには、ネットワークソースの追加 を参照してください。
- ネットワーク認証情報を追加するには、ネットワーク認証情報の追加 を参照してください。

ソースと認証情報、および Discovery でのそれらの使用方法の詳細は、次の情報を参照してください。

- ソースおよび認証情報について

ネットワーク上のアセットで Discovery が認証する方法の詳細は、以下の情報を参照してください。この情報には、権限を昇格したコマンドの実行に関するガイダンスが記載されています。これは、ネットワーク認証情報の設定時に行わないといけない場合があります。

- ネットワーク認証
- リモートネットワークアセットのスキャンで使用されるコマンド

3.1.1. ネットワークソースの追加

最初の Welcome ページまたは Sources ビューからソースを追加できます。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - Welcome ページから **Add Source** をクリックします。
   - Sources ビューから **Add** をクリックします。

   ソースの追加ウィザードが開きます。
2. Type ページで、**Network Range** をソースタイプとして選択し、**Next** をクリックします。
3. Credentials ページで、以下の情報を入力します。
   a. **Name** フィールドに、説明的な名前を入力します。
   b. **Search Addresses** フィールドに、1 つ以上のネットワーク識別子をコンマで区切って入力します。ホスト名、IP アドレス、および IP 範囲を入力できます。
      - ホスト名を DNS ホスト名として入力します (例: **server1.example.com)**。
      - CIDR または Ansible 表記で IP 範囲を入力します (例: CIDR 表記 **192.168.1.0/24**、Ansible 表記 **192.168.1.[1:254]**)。
   c. 必要に応じて、このソースのスキャンをデフォルトポート 22 で実行する必要がない場合は、**Port** フィールドに別のポートを入力します。
   d. **Credentials** リストで、このソースのネットワークリソースへのアクセスに必要な認証情報を選択します。必要な認証情報が存在しない場合は、**Add a credential** アイコンをクリックして Add Credential ウィザードを開きます。
   e. ネットワークリソースで、デフォルトの OpenSSH 実装ではなく、Ansible 接続メソッドが Python SSH 実装である必要がある場合は、デフォルトの OpenSSH 実装の代わりに、**Connect using Paramiko instead of OpenSSH** チェックボックスを選択します。
4. **Save** をクリックしてソースを保存し、**Close** をクリックして Add Source ウィザードを閉じます。

3.1.2. ネットワーク認証情報の追加

Credentials ビューから認証情報を追加するか、ソースの作成時に Add Source ウィザードから認証情報を追加できます。1 つのソースに含まれるすべてのアセットに認証するために、複数の認証情報を追加する必要がある場合があります。

前提条件

- ネットワーク認証情報に SSH 鍵認証タイプを使用する場合は、Discovery サーバーのインストール時に **/sshkeys** にマップされたディレクトリーにコピーする必要があります。このディレクトリーのデフォルトパスは **"${HOME}"/.local/share/discovery/sshkeys** です。**/sshkeys** ディレクトリーで使用できる SSH キーの詳細や、そのディレクトリーへのキーの追加を要求する場合は、Discovery サーバーを管理する管理者にお問い合わせください。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - Credentials ビューから、**Add → Network Credential** をクリックします。
   - Add Source ウィザードで、**Credentials** フィールドの **Add a credential** アイコンをクリックします。

   Add Credential ウィザードが開きます。
2. **Credential Name** フィールドに、説明的な名前を入力します。
3. **Authentication Type** フィールドで、使用する認証のタイプを選択します。**Username and Password** または **SSH Key** のいずれかを選択できます。
4. 認証タイプに応じて、適切なフィールドに認証データを入力します。
   - ユーザー名とパスワードの認証に、ユーザーのユーザー名とパスワードを入力します。このユーザーには、ネットワークまたはスキャンするネットワークのサブセットへの root レベルのアクセスが必要です。このユーザーは、選択した become メソッドを使用してルートレベルのアクセスを取得できるようにする必要があります。
   - SSH キー認証の場合は、ユーザー名と、Discovery サーバーコンテナーに対してローカルの SSH キーファイルへのパスを入力します。たとえば、キーファイルがサーバーの **"${HOME}"/.local/share/discovery/sshkeys** デフォルトパスにある場合は、そのパスを **SSH Key File** フィールドに入力します。パスフレーズの入力は任意です。
5. 特権の昇格の方法を入力します。ネットワークスキャン中に一部のコマンドを実行するには、権限の昇格が必要です。become メソッドのユーザー名およびパスワードの入力は任意です。
6. **Save** をクリックして認証情報を保存し、Add Credential ウィザードを閉じます。

3.1.3. ソースおよび認証情報について

スキャンを実行するには、ソースと認証情報の 2 つの基本的な構造のデータを設定する必要があります。スキャン中に検査するソースのタイプによって、ソースと認証情報の両方の設定に必要なデータのタイプが決まります。

ソース には、スキャン時に検査される単一のアセットまたは複数のアセットが含まれます。以下の 4 種類のソースを設定できます。

ネットワークソース

1つ以上の物理マシン、仮想マシン、またはコンテナー。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表現可能。

vCenter ソース

IT インフラストラクチャーのすべてまたは一部を管理する vCenter Server システム管理ソリューション。

Satellite ソース

IT インフラストラクチャーのすべてまたは一部を管理する Satellite システム管理ソリューション。

Red Hat OpenShift ソース

Red Hat OpenShift Container Platform ノードおよびワークロードのすべてまたは一部を管理する Red Hat OpenShift Container Platform クラスター。

Ansible ソース

Ansible ノードとワークロードを管理する Ansible 管理ソリューション。

Red Hat Advanced Cluster Security for Kubernetes ソース

Kubernetes 環境をセキュリティー保護する RHACS セキュリティープラットフォームソリューション。

ネットワークソースを使用している場合は、単一のソース内でグループ化する必要がある個々のアセットの数を決定します。現在、ネットワークソースに対してのみ、複数のアセットをソースに追加できます。次のリストには、ソースを追加するときに考慮する必要があるその他の要因がいくつか含まれています。

- アセットが開発、テスト、または本番環境の一部であるかどうか、およびコンピューティング能力の要求と同様の懸念がそれらのアセットの考慮事項であるかどうか。
- インストールされたソフトウェアへの頻繁な変更などの内部ビジネス慣習のために、特定のエンティティーまたはエンティティーのグループをより頻繁にスキャンするかどうか。

認証情報 は、ソースに含まれるアセットのすべてまたは一部でスキャンを実行する権限を持つユーザーのユーザー名やパスワード、SSH キーなどのデータが含まれます。ソースと同様に、認証情報はネットワーク、vCenter、Satellite、OpenShift、Ansible、または RHACS タイプとして設定されます。通常、ネットワークソースには、幅広い IP 範囲内の全アセットにアクセスするために多くの認証情報が必要になることが想定されるため、複数のネットワーク認証情報が必要になる場合があります。逆に、vCenter または Satellite ソースは、通常、必要に応じて単一の vCenter または Satellite 認証情報を使用して特定のシステム管理ソリューションサーバーにアクセスします。また、OpenShift、Ansible、または RHACS ソースは、単一のクラスターにアクセスするために単一の認証情報を使用します。

Sources ビューから新しいソースを追加でき、Credentials ビューから新しい認証情報を追加できます。ソースの作成中に、新しい認証情報を追加したり、既存の認証情報を選択したりすることもできます。認証情報をソースに直接関連付けるのは、ソースの作成時です。ソースと認証情報には一致するタイプが必要なため、ソースの作成時に追加する認証情報はソースと同じタイプを共有します。さらに、ソースの作成時に既存の認証情報を使用する場合は、利用可能な認証情報のリストに同じタイプの認証情報のみが含まれます。たとえば、ネットワークソースの作成時に利用できるのは、ネットワーク認証情報のみです。

3.1.4. ネットワーク認証

Discovery サーバーは、Ansible の SSH リモート接続機能を使用して、ネットワークスキャンのリモートシステムを検査します。ネットワーク認証情報を追加すると、ユーザー名とパスワードまたはユーザー名と SSH キーファイルのペアを使用して SSH 接続を設定します。リモートシステムが SSH キー認証を使用してアクセスされている場合は、パスフレーズを指定することもできます。

ネットワーク認証情報の設定時に、become メソッドを有効にすることもできます。become メソッドはスキャン中に権限の昇格に使用されます。これらの昇格された権限は、コマンドを実行し、スキャン

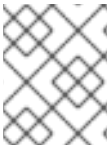
しているシステムのデータを取得するために必要です。スキャン中に、権限の昇格を必要としないコマンドの詳細は、リモートネットワークアセットのスキャンで使用されるコマンド を参照してください。

3.1.4.1. リモートネットワークアセットのスキャンで使用されるコマンド

ネットワークスキャンを実行する場合、Discovery では、ネットワーク内のリモートシステムで特定のコマンドを実行するために提供する認証情報を使用する必要があります。これらのコマンドの一部は、昇格された権限で実行する必要があります。このアクセスは、通常、**sudo** コマンドまたは同様のコマンドを使用して取得します。インストールされた製品に関するレポートを作成するために Discovery が使用するファクトのタイプを収集するには、昇格された特権が必要です。

権限を昇格せずにネットワークソースのスキャンを実行することは可能ですが、スキャンの結果が不完全になります。ネットワークスキャンの不完全な結果は、スキャンに対して生成されたレポートの質に影響します。

以下の情報には、ネットワークスキャン中にリモートホストで Discovery を実行するコマンドが記載されています。情報には、権限を昇格せずに実行できる基本的なコマンドと、レポートに対して最も正確で完全な情報を収集するために昇格した権限で実行する必要があるコマンドが含まれます。



注記

次のコマンドの他に、Discovery は **bash** シェルが提供するような標準のシェル機能にも左右されます。

3.1.4.1.1. 権限の昇格を必要としない基本コマンド

以下のコマンドでは、スキャン中にファクトを収集するのに、昇格した権限は必要ありません。

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

- tune2fs
- xargs

3.1.4.1.2. 権限の昇格が必要なコマンド

以下のコマンドには、スキャン中にファクトを収集するのに昇格した権限が必要になります。各コマンドには、スキャン中に Discovery が試行する個々のファクトまたはファクトのカテゴリーの一覧が含まれます。これらのファクトは、そのコマンドで昇格した権限が利用できない場合にレポートに含めることができません。

- 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. SATELLITE ソースおよび認証情報の追加

Red Hat Satellite Server デプロイメントでスキャンを実行するには、スキャンする Satellite Server サーバーを識別するソースを追加する必要があります。その後、そのサーバーにアクセスするために認証データが含まれる認証情報を追加する必要があります。

詳細情報

Satellite ソースおよび認証情報を追加して、Satellite Server のスキャンに必要な情報を提供します。詳細は、以下の情報を参照してください。

- サテライトソースを追加するには、サテライトソースの追加 を参照してください。
- サテライト認証情報を追加するには、サテライト認証情報の追加 を参照してください。

ソースと認証情報、および Discovery でのそれらの使用方法の詳細は、次の情報を参照してください。

- ソースおよび認証情報について

Satellite Server サーバーで Discovery が認証する方法の詳細は、以下の情報を参照してください。この情報には、証明書の検証に関するガイダンスと、サテライト認証情報の設定中に行う必要がある SSL 通信の選択肢が含まれます。

- Satellite Server の認証

3.2.1. Satellite ソースの追加

最初の Welcome ページまたは Sources ビューからソースを追加できます。

手順

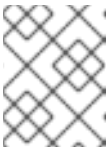
1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - Welcome ページから **Add Source** をクリックします。
   - Sources ビューから **Add** をクリックします。

   ソースの追加ウィザードが開きます。
2. Type ページで、**Satellite** をソースタイプとして選択し、**Next** をクリックします。
3. Credentials ページで、以下の情報を入力します。
   a. **Name** フィールドに、説明的な名前を入力します。

b. **IP Address or Hostname** フィールドに、このソースの Satellite サーバーの IP アドレスまたはホスト名を入力します。このソースのスキャンをデフォルトのポート 443 で実行しない場合は、別のポートを入力します。たとえば、Satellite サーバーの IP アドレスが 192.0.2.15 で、ポートを 80 に変更する場合は、**192.0.2.15:80** を入力します。

c. **Credentials** リストで、このソースの Satellite サーバーへのアクセスに必要な認証情報を選択します。必要な認証情報が存在しない場合は、**Add a credential** アイコンをクリックして Add Credential ウィザードを開きます。

d. **Connection** リストで、このソースのスキャン中にセキュアな接続に使用される SSL プロトコルを選択します。



注記

Satellite Server は、SSL の無効化をサポートしません。**Disable SSL** オプションを選択すると、このオプションは無視されます。

e. Satellite サーバーの SSL 検証をアップグレードして、認証局から検証された SSL 証明書を確認する必要がある場合は、**Verify SSL Certificate** チェックボックスを選択します。

4. **Save** をクリックしてソースを保存し、**Close** をクリックして Add Source ウィザードを閉じます。

3.2.2. Satellite 認証情報の追加

Credentials ビューから認証情報を追加するか、ソースの作成時に Add Source ウィザードから認証情報を追加できます。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。

   - Credentials ビューから、**Add → Satellite Credential** をクリックします。
   - Add Source ウィザードで、**Credentials** フィールドの **Add a credential** アイコンをクリックします。

   Add Credential ウィザードが開きます。

2. **Credential Name** フィールドに、説明的な名前を入力します。
3. Satellite Server 管理者のユーザー名とパスワードを入力します。
4. **Save** をクリックして認証情報を保存し、Add Credential ウィザードを閉じます。

3.2.3. ソースおよび認証情報について

スキャンを実行するには、ソースと認証情報の 2 つの基本的な構造のデータを設定する必要があります。スキャン中に検査するソースのタイプによって、ソースと認証情報の両方の設定に必要なデータのタイプが決まります。

ソース には、スキャン時に検査される単一のアセットまたは複数のアセットが含まれます。以下の 4 種類のソースを設定できます。

ネットワークソース

1 つ以上の物理マシン、仮想マシン、またはコンテナー。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表現可能。

vCenter ソース

IT インフラストラクチャーのすべてまたは一部を管理する vCenter Server システム管理ソリューション。

Satellite ソース

IT インフラストラクチャーのすべてまたは一部を管理する Satellite システム管理ソリューション。

Red Hat OpenShift ソース

Red Hat OpenShift Container Platform ノードおよびワークロードのすべてまたは一部を管理する Red Hat OpenShift Container Platform クラスター。

Ansible ソース

Ansible ノードとワークロードを管理する Ansible 管理ソリューション。

Red Hat Advanced Cluster Security for Kubernetes ソース

Kubernetes 環境をセキュリティー保護する RHACS セキュリティープラットフォームソリューション。

ネットワークソースを使用している場合は、単一のソース内でグループ化する必要がある個々のアセットの数を決定します。現在、ネットワークソースに対してのみ、複数のアセットをソースに追加できます。次のリストには、ソースを追加するときに考慮する必要があるその他の要因がいくつか含まれています。

- アセットが開発、テスト、または本番環境の一部であるかどうか、およびコンピューティング能力の要求と同様の懸念がそれらのアセットの考慮事項であるかどうか。
- インストールされたソフトウェアへの頻繁な変更などの内部ビジネス慣習のために、特定のエンティティーまたはエンティティーのグループをより頻繁にスキャンするかどうか。

認証情報 は、ソースに含まれるアセットのすべてまたは一部でスキャンを実行する権限を持つユーザーのユーザー名やパスワード、SSH キーなどのデータが含まれます。ソースと同様に、認証情報はネットワーク、vCenter、Satellite、OpenShift、Ansible、または RHACS タイプとして設定されます。通常、ネットワークソースには、幅広い IP 範囲内の全アセットにアクセスするために多くの認証情報が必要になることが想定されるため、複数のネットワーク認証情報が必要になる場合があります。逆に、vCenter または Satellite ソースは、通常、必要に応じて単一の vCenter または Satellite 認証情報を使用して特定のシステム管理ソリューションサーバーにアクセスします。また、OpenShift、Ansible、または RHACS ソースは、単一のクラスターにアクセスするために単一の認証情報を使用します。

Sources ビューから新しいソースを追加でき、Credentials ビューから新しい認証情報を追加できます。ソースの作成中に、新しい認証情報を追加したり、既存の認証情報を選択したりすることもできます。認証情報をソースに直接関連付けるのは、ソースの作成時です。ソースと認証情報には一致するタイプが必要なため、ソースの作成時に追加する認証情報はソースと同じタイプを共有します。さらに、ソースの作成時に既存の認証情報を使用する場合は、利用可能な認証情報のリストに同じタイプの認証情報のみが含まれます。たとえば、ネットワークソースの作成時に利用できるのは、ネットワーク認証情報のみです。

3.2.4. Satellite Server の認証

Satellite のスキャンでは、Satellite Server への接続とアクセスは、HTTPS 経由で暗号化される Basic 認証 (ユーザー名とパスワード) から派生します。デフォルトでは、Satellite スキャンは SSL (Secure Sockets Layer) プロトコルを介して証明書の検証とセキュアな通信で実行されます。ソースの作成時に、証明書の検証およびセキュアな通信に使用する複数の異なる SSL プロトコルおよび TLS (Transport Layer Security) プロトコルから選択できます。

スキャン中に Satellite サーバーに適切に接続するために、証明書検証のレベルを調整する必要がある場

合があります。たとえば、Satellite サーバーは、認証局から検証された SSL 証明書を使用する場合があります。ソースの作成時に、SSL 証明書の検証をアップグレードして、そのソースのスキャン中にその証明書を確認することができます。この場合、Satellite サーバーは自己署名証明書を使用する場合があります。ソースの作成時に、SSL 検証をデフォルトのままにし、そのソースのスキャンが証明書をチェックしないようにできます。このように、自己署名証明書を使用する場合にオプションをデフォルトのままにすることで、スキャンエラーを回避できる可能性があります。

現在、SSL を無効にするオプションはインターフェイスで利用できますが、Satellite Server では SSL の無効化をサポートしていません。サテライトソースの作成時に **Disable SSL** オプションを選択すると、このオプションは無視されます。

3.3. VCENTER ソースおよび認証情報の追加

vCenter Server デプロイメントでスキャンを実行するには、スキャンする vCenter Server サーバーを識別するソースを追加する必要があります。その後、そのサーバーにアクセスするために認証データが含まれる認証情報を追加する必要があります。

詳細情報

vCenter ソースおよび認証情報を追加し、vCenter Server をスキャンするために必要な情報を提供します。詳細は、以下の情報を参照してください。

- vCenter ソースを追加するには、vCenter ソースの追加 を参照してください。
- vCenter 認証情報を追加するには、vCenter の認証情報の追加 を参照してください。

ソースと認証情報、および Discovery でのそれらの使用方法の詳細は、次の情報を参照してください。

- ソースおよび認証情報について

vCenter Server サーバーで Discovery が認証する方法の詳細は、以下の情報を参照してください。この情報には、証明書の検証に関するガイダンスと、vCenter の認証情報設定中に行う必要がある SSL 通信の選択肢が含まれます。

- vCenter Server の認証

3.3.1. vCenter ソースの追加

最初の Welcome ページまたは Sources ビューからソースを追加できます。

注記

vCenter ソースは、vCenter デプロイメントとだけ互換性があります。このソースを使用する場合に、Red Hat によってサポートされているものであっても、他の仮想化インフラストラクチャーをスキャンすることはできません。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - Welcome ページから **Add Source** をクリックします。
   - Sources ビューから **Add** をクリックします。

   ソースの追加ウィザードが開きます。

2. Type ページで **vCenter Server** をソースタイプとして選択し、**Next** をクリックします。

3. Credentials ページで、以下の情報を入力します。

   a. **Name** フィールドに、説明的な名前を入力します。

   b. **IP Address or Hostname** フィールドに、このソースの vCenter Server の IP アドレスまたはホスト名を入力します。このソースのスキャンをデフォルトのポート 443 で実行しない場合は、別のポートを入力します。たとえば、vCenter Server の IP アドレスが 192.0.2.15 で、ポートを 80 に変更する場合は、**192.0.2.15:80** を入力します。

   c. **Credentials** リストで、このソースの vCenter Server へのアクセスに必要な認証情報を選択します。必要な認証情報が存在しない場合は、**Add a credential** アイコンをクリックして Add Credential ウィザードを開きます。

   d. **Connection** リストで、このソースのスキャン中にセキュアな接続に使用される SSL プロトコルを選択します。**Disable SSL** を選択して、このソースのスキャン時にセキュアな通信を無効にします。

   e. vCenter Server の SSL 検証をアップグレードして、認証局から検証された SSL 証明書を確認する必要がある場合は、**Verify SSL Certificate** チェックボックスを選択します。

4. **Save** をクリックしてソースを保存し、**Close** をクリックして Add Source ウィザードを閉じます。

3.3.2. vCenter 認証情報の追加

Credentials ビューから認証情報を追加するか、ソースの作成時に Add Source ウィザードから認証情報を追加できます。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。

   - Credentials ビューで **Add → VCenter Credential** をクリックします。
   - Add Source ウィザードで、**Credentials** フィールドの **Add a credential** アイコンをクリックします。

   Add Credential ウィザードが開きます。

2. **Credential Name** フィールドに、説明的な名前を入力します。

3. vCenter Server 管理者のユーザー名およびパスワードを入力します。

4. **Save** をクリックして認証情報を保存し、Add Credential ウィザードを閉じます。

3.3.3. ソースおよび認証情報について

スキャンを実行するには、ソースと認証情報の 2 つの基本的な構造のデータを設定する必要があります。スキャン中に検査するソースのタイプによって、ソースと認証情報の両方の設定に必要なデータのタイプが決まります。

ソース には、スキャン時に検査される単一のアセットまたは複数のアセットが含まれます。以下の 4 種類のソースを設定できます。

ネットワークソース

1つ以上の物理マシン、仮想マシン、またはコンテナー。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表現可能。

vCenter ソース

IT インフラストラクチャーのすべてまたは一部を管理する vCenter Server システム管理ソリューション。

Satellite ソース

IT インフラストラクチャーのすべてまたは一部を管理する Satellite システム管理ソリューション。

Red Hat OpenShift ソース

Red Hat OpenShift Container Platform ノードおよびワークロードのすべてまたは一部を管理する Red Hat OpenShift Container Platform クラスター。

Ansible ソース

Ansible ノードとワークロードを管理する Ansible 管理ソリューション。

Red Hat Advanced Cluster Security for Kubernetes ソース

Kubernetes 環境をセキュリティー保護する RHACS セキュリティープラットフォームソリューション。

ネットワークソースを使用している場合は、単一のソース内でグループ化する必要がある個々のアセットの数を決定します。現在、ネットワークソースに対してのみ、複数のアセットをソースに追加できます。次のリストには、ソースを追加するときに考慮する必要があるその他の要因がいくつか含まれています。

- アセットが開発、テスト、または本番環境の一部であるかどうか、およびコンピューティング能力の要求と同様の懸念がそれらのアセットの考慮事項であるかどうか。
- インストールされたソフトウェアへの頻繁な変更などの内部ビジネス慣習のために、特定のエンティティーまたはエンティティーのグループをより頻繁にスキャンするかどうか。

認証情報 は、ソースに含まれるアセットのすべてまたは一部でスキャンを実行する権限を持つユーザーのユーザー名やパスワード、SSH キーなどのデータが含まれます。ソースと同様に、認証情報はネットワーク、vCenter、Satellite、OpenShift、Ansible、または RHACS タイプとして設定されます。通常、ネットワークソースには、幅広い IP 範囲内の全アセットにアクセスするために多くの認証情報が必要になることが想定されるため、複数のネットワーク認証情報が必要になる場合があります。逆に、vCenter または Satellite ソースは、通常、必要に応じて単一の vCenter または Satellite 認証情報を使用して特定のシステム管理ソリューションサーバーにアクセスします。また、OpenShift、Ansible、または RHACS ソースは、単一のクラスターにアクセスするために単一の認証情報を使用します。

Sources ビューから新しいソースを追加でき、Credentials ビューから新しい認証情報を追加できます。ソースの作成中に、新しい認証情報を追加したり、既存の認証情報を選択したりすることもできます。認証情報をソースに直接関連付けるのは、ソースの作成時です。ソースと認証情報には一致するタイプが必要なため、ソースの作成時に追加する認証情報はソースと同じタイプを共有します。さらに、ソースの作成時に既存の認証情報を使用する場合は、利用可能な認証情報のリストに同じタイプの認証情報のみが含まれます。たとえば、ネットワークソースの作成時に利用できるのは、ネットワーク認証情報のみです。

3.3.4. vCenter Server の認証

vCenter スキャンでは、vCenter Server への接続とアクセスは、HTTPS 経由で暗号化される Basic 認証 (ユーザー名とパスワード) から派生します。デフォルトでは、vCenter スキャンは、SSL (Secure Sockets Layer) プロトコルを介して証明書の検証とセキュアな通信で実行されます。ソースの作成時に、証明書の検証およびセキュアな通信に使用する複数の異なる SSL プロトコルおよび TLS (Transport Layer Security) プロトコルから選択できます。

スキャン中に vCenter サーバーに適切に接続できるように、証明書検証のレベルの調整しが必要な場合

があります。たとえば、vCenter サーバーは認証局から検証された SSL 証明書を使用する可能性があります。ソースの作成時に、SSL 証明書の検証をアップグレードして、そのソースのスキャン中にその証明書を確認することができます。vCenter サーバーが自己署名証明書を使用する可能性があります。ソースの作成時に、SSL 検証をデフォルトのままにし、そのソースのスキャンが証明書をチェックしないようにできます。このように、自己署名証明書を使用する場合にオプションをデフォルトのままにすることで、スキャンエラーを回避できる可能性があります。

vCenter サーバーが Web アプリケーションに SSL 通信を使用するように設定されていない場合は、スキャン時に SSL をセキュア通信メソッドとして無効にする必要もあります。たとえば、HTTP をポート 80 で使用して、vCenter サーバーが Web アプリケーションと通信するように設定できます。その場合は、ソースの作成中に、そのソースのスキャンに対して SSL 通信を無効にできます。

3.4. OPENSHIFT ソースおよび認証情報の追加

Red Hat OpenShift Container Platform デプロイメントでスキャンを実行するには、スキャンする Red Hat OpenShift Container Platform クラスターを識別するソースを追加する必要があります。その後、そのクラスターにアクセスするために認証データが含まれる認証情報を追加する必要があります。

詳細情報

OpenShift ソースおよび認証情報を追加して、Red Hat OpenShift Container Platform クラスターのスキャンに必要な情報を提供します。詳細は、以下の情報を参照してください。

- OpenShift ソースを追加するには、OpenShift ソースの追加 を参照してください。
- OpenShift 認証情報を追加するには、OpenShift 認証情報の追加 を参照してください。

ソースと認証情報、および Discovery でのそれらの使用方法の詳細は、次の情報を参照してください。

- ソースおよび認証情報について

Red Hat OpenShift Container Platform クラスターで Discovery が認証する方法の詳細は、以下の情報を参照してください。この情報には、証明書の検証に関するガイダンスと、OpenShift の認証情報設定中に行う必要がある SSL 通信の選択肢が含まれます。

- Red Hat OpenShift Container Platform 認証

3.4.1. Red Hat OpenShift Container Platform ソースの追加

最初の Welcome ページまたは Sources ビューからソースを追加できます。

前提条件

- Red Hat OpenShift Container Platform Web コンソールの管理者パースペクティブにアクセスし、API アドレスおよびトークンの値を取得できる。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - Welcome ページから **Add Source** をクリックします。
   - Sources ビューから **Add** をクリックします。

   ソースの追加ウィザードが開きます。

2. Type ページで、**OpenShift** をソースタイプとして選択し、**Next** をクリックします。

3. Credentials ページで、以下の情報を入力します。

   a. **Name** フィールドに、説明的な名前を入力します。

   b. **IP Address or Hostname** フィールドに、このソースの Red Hat OpenShift Container Platform クラスター API アドレスを入力します。Web コンソールでクラスターの概要の詳細を表示すると、クラスター API アドレスを確認できます。

   c. **Credentials** 一覧で、このソースのクラスターへのアクセスに必要な認証情報を選択します。必要な認証情報が存在しない場合は、**Add a credential** アイコンをクリックして Add Credential ウィザードを開きます。

   d. **Connection** リストで、このソースのスキャン中にセキュアな接続に使用される SSL プロトコルを選択します。**Disable SSL** を選択して、このソースのスキャン時にセキュアな通信を無効にします。

   e. クラスターの SSL 検証をアップグレードして、認証局から検証された SSL 証明書を確認する必要がある場合は、**Verify SSL Certificate** チェックボックスを選択します。

4. **Save** をクリックしてソースを保存し、**Close** をクリックして Add Source ウィザードを閉じます。

3.4.2. Red Hat OpenShift Container Platform 認証情報の追加

Credentials ビューから認証情報を追加するか、ソースの作成時に Add Source ウィザードから認証情報を追加できます。

前提条件

- Red Hat OpenShift Container Platform Web コンソールの管理者パースペクティブにアクセスし、API アドレスおよびトークンの値を取得できる。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。

   - Credentials ビューから、**Add → OpenShift** をクリックします。

   - Add Source ウィザードで、**Credentials** フィールドの **Add a credential** アイコンをクリックします。

   Add Credential ウィザードが開きます。

2. **Credential Name** フィールドに、説明的な名前を入力します。

3. 管理者コンソールから Red Hat OpenShift Container Platform クラスターの API トークンを入力します。コンソールでユーザー名をクリックし、**Display Token** オプションをクリックして、**Your API token is** に表示されている値をコピーすると、API トークンを見つけることができます。

4. **Save** をクリックして認証情報を保存し、Add Credential ウィザードを閉じます。

3.4.3. ソースおよび認証情報について

スキャンを実行するには、ソースと認証情報の 2 つの基本的な構造のデータを設定する必要があります。スキャン中に検査するソースのタイプによって、ソースと認証情報の両方の設定に必要なデータのタイプが決まります。

ソース には、スキャン時に検査される単一のアセットまたは複数のアセットが含まれます。以下の 4 種類のソースを設定できます。

ネットワークソース

1 つ以上の物理マシン、仮想マシン、またはコンテナー。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表現可能。

vCenter ソース

IT インフラストラクチャーのすべてまたは一部を管理する vCenter Server システム管理ソリューション。

Satellite ソース

IT インフラストラクチャーのすべてまたは一部を管理する Satellite システム管理ソリューション。

Red Hat OpenShift ソース

Red Hat OpenShift Container Platform ノードおよびワークロードのすべてまたは一部を管理する Red Hat OpenShift Container Platform クラスター。

Ansible ソース

Ansible ノードとワークロードを管理する Ansible 管理ソリューション。

Red Hat Advanced Cluster Security for Kubernetes ソース

Kubernetes 環境をセキュリティー保護する RHACS セキュリティープラットフォームソリューション。

ネットワークソースを使用している場合は、単一のソース内でグループ化する必要がある個々のアセットの数を決定します。現在、ネットワークソースに対してのみ、複数のアセットをソースに追加できます。次のリストには、ソースを追加するときに考慮する必要があるその他の要因がいくつか含まれています。

- アセットが開発、テスト、または本番環境の一部であるかどうか、およびコンピューティング能力の要求と同様の懸念がそれらのアセットの考慮事項であるかどうか。
- インストールされたソフトウェアへの頻繁な変更などの内部ビジネス慣習のために、特定のエンティティーまたはエンティティーのグループをより頻繁にスキャンするかどうか。

認証情報 は、ソースに含まれるアセットのすべてまたは一部でスキャンを実行する権限を持つユーザーのユーザー名やパスワード、SSH キーなどのデータが含まれます。ソースと同様に、認証情報はネットワーク、vCenter、Satellite、OpenShift、Ansible、または RHACS タイプとして設定されます。通常、ネットワークソースには、幅広い IP 範囲内の全アセットにアクセスするために多くの認証情報が必要になることが想定されるため、複数のネットワーク認証情報が必要になる場合があります。逆に、vCenter または Satellite ソースは、通常、必要に応じて単一の vCenter または Satellite 認証情報を使用して特定のシステム管理ソリューションサーバーにアクセスします。また、OpenShift、Ansible、または RHACS ソースは、単一のクラスターにアクセスするために単一の認証情報を使用します。

Sources ビューから新しいソースを追加でき、Credentials ビューから新しい認証情報を追加できます。ソースの作成中に、新しい認証情報を追加したり、既存の認証情報を選択したりすることもできます。認証情報をソースに直接関連付けるのは、ソースの作成時です。ソースと認証情報には一致するタイプが必要なため、ソースの作成時に追加する認証情報はソースと同じタイプを共有します。さらに、ソースの作成時に既存の認証情報を使用する場合は、利用可能な認証情報のリストに同じタイプの認証情報のみが含まれます。たとえば、ネットワークソースの作成時に利用できるのは、ネットワーク認証情報のみです。

3.4.4. Red Hat OpenShift Container Platform 認証

OpenShift スキャンでは、OpenShift クラスター API アドレスへの接続およびアクセスは、クラスター API アドレスと HTTPS で暗号化される API トークンを使用した Basic 認証から派生します。デフォルトでは、OpenShift スキャンは、SSL (Secure Sockets Layer) プロトコルを介して証明書の検証とセキュアな通信で実行されます。ソースの作成時に、証明書の検証およびセキュアな通信に使用する複数の異なる SSL プロトコルおよび TLS (Transport Layer Security) プロトコルから選択できます。

スキャン中に Red Hat OpenShift Container Platform クラスター API アドレスに適切に接続できるように、証明書検証のレベルを調整する必要がある場合があります。たとえば、OpenShift クラスター API アドレスは、認証局からの検証済み SSL 証明書を使用する場合があります。ソースの作成時に、SSL 証明書の検証をアップグレードして、そのソースのスキャン中にその証明書を確認することができます。逆に、クラスター API アドレスが自己署名証明書を使用する場合もあります。ソースの作成時に、SSL 検証をデフォルトのままにし、そのソースのスキャンが証明書をチェックしないようにできます。このように、自己署名証明書を使用する場合にオプションをデフォルトのままにすることで、スキャンエラーを回避できる可能性があります。

Web アプリケーションで SSL 通信を使用するように OpenShift クラスター API アドレスが設定されていない場合は、スキャン時にセキュアな通信方法である SSL を無効にしないといけない場合もあります。たとえば、OpenShift サーバーが、ポート 80 で HTTP を使用して Web アプリケーションと通信するように設定されている場合があります。その場合は、ソースの作成中に、そのソースのスキャンに対して SSL 通信を無効にできます。

3.5. ANSIBLE ソースと認証情報の追加

Ansible デプロイメントでスキャンを実行するには、スキャンする Ansible Automation Platform を識別するソースを追加する必要があります。その後、そのクラスターにアクセスするために認証データが含まれる認証情報を追加する必要があります。

詳細情報

Ansible ソースと認証情報を追加して、Ansible Automation Platform デプロイメントのスキャンに必要な情報を提供します。詳細は、以下の情報を参照してください。

- Ansible ソースを追加するには、Add an Ansible source を参照してください。
- Ansible 認証情報を追加するには、 Add an Ansible credential を参照してください。

ソースと認証情報、および Discovery でのそれらの使用方法の詳細は、次の情報を参照してください。

- ソースおよび認証情報について

Ansible デプロイメントで Discovery が認証される方法の詳細は、次の情報を参照してください。この情報には、Ansible 認証情報の設定時に必要になる可能性のある、証明書の検証と SSL 通信の選択に関するガイダンスが含まれています。

- Ansible Automation Platform

3.5.1. Red Hat Ansible Automation Platform ソースの追加

最初の Welcome ページまたは Sources ビューからソースを追加できます。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。

- Welcome ページから **Add Source** をクリックします。
- Sources ビューから **Add Source** をクリックします。

ソースの追加ウィザードが開きます。

2. Type ページで、ソースタイプとして **Ansible Controller** を選択し、**Next** をクリックします。
3. Credentials ページで、以下の情報を入力します。
   a. **Name** フィールドに、説明的な名前を入力します。
   b. **IP Address or Hostname** フィールドに、このソースの Ansible ホスト IP アドレスを入力します。ポータルでコントローラーの概要の詳細を表示すると、ホスト IP アドレスを見つけることができます。
   c. **Credentials** 一覧で、このソースのクラスターへのアクセスに必要な認証情報を選択します。必要な認証情報が存在しない場合は、**Add a credential** アイコンをクリックして Add Credential ウィザードを開きます。
   d. **Connection** リストで、このソースのスキャン中にセキュアな接続に使用される SSL プロトコルを選択します。**Disable SSL** を選択して、このソースのスキャン時にセキュアな通信を無効にします。
   e. クラスターの SSL 検証をアップグレードして、認証局から検証された SSL 証明書を確認する必要がある場合は、**Verify SSL Certificate** チェックボックスを選択します。
4. **Save** をクリックしてソースを保存し、**Close** をクリックして Add Source ウィザードを閉じます。

3.5.2. Red Hat Ansible Automation Platform 認証情報の追加

Credentials ビューから認証情報を追加するか、ソースの作成時に Add Source ウィザードから認証情報を追加できます。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - 認証情報ビューで、**Add → Ansible Credential** をクリックします。
   - Add Source ウィザードで、**Credentials** フィールドの **Add a credential** アイコンをクリックします。

   Add Credential ウィザードが開きます。
2. **Credential Name** フィールドに、説明的な名前を入力します。
3. **User Name** フィールドに、Ansible コントローラーインスタンスのユーザー名を入力します。
4. **Password** フィールドに、Ansible Controller インスタンスのパスワードを入力します。
5. **Save** をクリックして認証情報を保存します。Add Credential ウィザードが閉じます。

3.5.3. ソースおよび認証情報について

スキャンを実行するには、ソースと認証情報の 2 つの基本的な構造のデータを設定する必要があります。スキャン中に検査するソースのタイプによって、ソースと認証情報の両方の設定に必要なデータのタイプが決まります。

ソース には、スキャン時に検査される単一のアセットまたは複数のアセットが含まれます。以下の 4 種類のソースを設定できます。

ネットワークソース

1つ以上の物理マシン、仮想マシン、またはコンテナー。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表現可能。

vCenter ソース

IT インフラストラクチャーのすべてまたは一部を管理する vCenter Server システム管理ソリューション。

Satellite ソース

IT インフラストラクチャーのすべてまたは一部を管理する Satellite システム管理ソリューション。

Red Hat OpenShift ソース

Red Hat OpenShift Container Platform ノードおよびワークロードのすべてまたは一部を管理する Red Hat OpenShift Container Platform クラスター。

Ansible ソース

Ansible ノードとワークロードを管理する Ansible 管理ソリューション。

Red Hat Advanced Cluster Security for Kubernetes ソース

Kubernetes 環境をセキュリティー保護する RHACS セキュリティープラットフォームソリューション。

ネットワークソースを使用している場合は、単一のソース内でグループ化する必要がある個々のアセットの数を決定します。現在、ネットワークソースに対してのみ、複数のアセットをソースに追加できます。次のリストには、ソースを追加するときに考慮する必要があるその他の要因がいくつか含まれています。

- アセットが開発、テスト、または本番環境の一部であるかどうか、およびコンピューティング能力の要求と同様の懸念がそれらのアセットの考慮事項であるかどうか。
- インストールされたソフトウェアへの頻繁な変更などの内部ビジネス慣習のために、特定のエンティティーまたはエンティティーのグループをより頻繁にスキャンするかどうか。

認証情報 は、ソースに含まれるアセットのすべてまたは一部でスキャンを実行する権限を持つユーザーのユーザー名やパスワード、SSH キーなどのデータが含まれます。ソースと同様に、認証情報はネットワーク、vCenter、Satellite、OpenShift、Ansible、または RHACS タイプとして設定されます。通常、ネットワークソースには、幅広い IP 範囲内の全アセットにアクセスするために多くの認証情報が必要になることが想定されるため、複数のネットワーク認証情報が必要になる場合があります。逆に、vCenter または Satellite ソースは、通常、必要に応じて単一の vCenter または Satellite 認証情報を使用して特定のシステム管理ソリューションサーバーにアクセスします。また、OpenShift、Ansible、または RHACS ソースは、単一のクラスターにアクセスするために単一の認証情報を使用します。

Sources ビューから新しいソースを追加でき、Credentials ビューから新しい認証情報を追加できます。ソースの作成中に、新しい認証情報を追加したり、既存の認証情報を選択したりすることもできます。認証情報をソースに直接関連付けるのは、ソースの作成時です。ソースと認証情報には一致するタイプが必要なため、ソースの作成時に追加する認証情報はソースと同じタイプを共有します。さらに、ソースの作成時に既存の認証情報を使用する場合は、利用可能な認証情報のリストに同じタイプの認証情報のみが含まれます。たとえば、ネットワークソースの作成時に利用できるのは、ネットワーク認証情報のみです。

3.5.4. Ansible 認証

Ansible スキャンの場合、Ansible ホスト IP アドレスへの接続とアクセスは、ホスト IP アドレスと HTTPS 経由で暗号化されたパスワードによる基本認証に基づいています。デフォルトでは、Ansible スキャンは証明書の検証と SSL (Secure Sockets Layer) プロトコルを介した安全な通信を使用して実行されます。ソースの作成時に、証明書の検証およびセキュアな通信に使用する複数の異なる SSL プロトコルおよび TLS (Transport Layer Security) プロトコルから選択できます。

スキャン中に Ansible ホストの IP アドレスに適切に接続するには、証明書検証のレベルを調整する必要がある場合があります。たとえば、Ansible ホストの IP アドレスは、認証局からの検証済み SSL 証明書を使用する場合があります。ソースの作成時に、SSL 証明書の検証をアップグレードして、そのソースのスキャン中にその証明書を確認することができます。逆に、ホスト IP アドレスでは自己署名証明書が使用される場合があります。ソースの作成時に、SSL 検証をデフォルトのままにし、そのソースのスキャンが証明書をチェックしないようにできます。このように、自己署名証明書を使用する場合にオプションをデフォルトのままにすることで、スキャンエラーを回避できる可能性があります。

Ansible ホスト IP アドレスが Web アプリケーションに SSL 通信を使用するように設定されていない場合は、スキャン中に安全な通信方法として SSL を無効にする必要がある場合もあります。たとえば、Ansible ホストの IP アドレスは、ポート 80 で HTTP を使用して Web アプリケーションと通信するように設定されている場合があります。その場合は、ソースの作成中に、そのソースのスキャンに対して SSL 通信を無効にできます。

3.6. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES ソースと認証情報の追加

Red Hat Advanced Cluster Security for Kubernetes (RHACS) デプロイメントでスキャンを実行するには、スキャンする RHACS インスタンスを識別するソースを追加する必要があります。その後、そのインスタンスにアクセスするために認証データが含まれる認証情報を追加する必要があります。

詳細情報

RHACS ソースと認証情報を追加して、RHACS インスタンスをスキャンするために必要な情報を提供します。詳細は、以下の情報を参照してください。

- RHACS ソースを追加するには、RHACS ソースの追加 を参照してください。
- RHACS 認証情報を追加するには、RHACS 認証情報の追加 を参照してください。

ソースと認証情報、および Discovery でのそれらの使用方法の詳細は、次の情報を参照してください。

- ソースおよび認証情報について

Red Hat Advanced Cluster Security for Kubernetes インスタンスで Discovery が認証する方法の詳細は、以下の情報を参照してください。この情報には、RHACS 認証情報の設定時に必要になる可能性のある、証明書の検証と SSL 通信の選択に関するガイダンスが含まれています。

- Kubernetes 用 Red Hat Advanced Cluster Security

3.6.1. Red Hat Advanced Cluster Security for Kubernetes ソースの追加

最初の Welcome ページまたは Sources ビューからソースを追加できます。

前提条件

- Red Hat Advanced Cluster Security for Kubernetes (RHACS) ポータルにアクセスし、管理 API トークンの値を生成できる。

- RHACS ポータルにアクセスして RHACS Central エンドポイントを見つけることができるか、RHACS Configuration Management Cloud Service インスタンスの詳細にアクセスできる。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。
   - Welcome ページから **Add Source** をクリックします。
   - Sources ビューから **Add** をクリックします。

   ソースの追加ウィザードが開きます。
2. Type ページで、**RHACS** をソースタイプとして選択し、**Next** をクリックします。
3. Credentials ページで、以下の情報を入力します。
   a. **Name** フィールドに、説明的な名前を入力します。
   b. **IP Address or Hostname** フィールドに、このソースの Red Hat Advanced Cluster Security for Kubernetes Central アドレスを入力します。
      - RHACS が OpenShift にデプロイされている場合は、クラスターのネットワークルートを表示することでアドレスを見つけることができます。
      - RHACS がクラウド上にデプロイされている場合は、インスタンスの詳細でこの情報を見つけることができます。
   c. **Credentials** 一覧で、このソースのクラスターへのアクセスに必要な認証情報を選択します。必要な認証情報が存在しない場合は、**Add a credential** アイコンをクリックして Add Credential ウィザードを開きます。
   d. **Connection** リストで、このソースのスキャン中にセキュアな接続に使用される SSL プロトコルを選択します。**Disable SSL** を選択して、このソースのスキャン時にセキュアな通信を無効にします。
   e. クラスターの SSL 検証をアップグレードして、認証局から検証された SSL 証明書を確認する必要がある場合は、**Verify SSL Certificate** チェックボックスを選択します。
4. **Save** をクリックしてソースを保存し、**Close** をクリックして Add Source ウィザードを閉じます。

3.6.2. RHACS 認証情報の追加

Credentials ビューから認証情報を追加するか、ソースの作成時に Add Source ウィザードから認証情報を追加できます。

前提条件

- Red Hat Advanced Cluster Security for Kubernetes (RHACS) ポータルにアクセスし、管理 API トークンの値を生成できる。
- RHACS ポータルにアクセスして RHACS Central エンドポイントを見つけることができるか、RHACS Configuration Management Cloud Service インスタンスの詳細にアクセスできる。

手順

1. オプションをクリックして、場所に基づいて新しい認証情報を追加します。

   - Credentials ビューから、**Add → RHACS** をクリックします。
   - Add Source ウィザードで、**Credentials** フィールドの **Add a credential** アイコンをクリックします。

   Add Credential ウィザードが開きます。

2. **Credential Name** フィールドに、説明的な名前を入力します。
3. RHACS ポータルから RHACS の API トークンを入力します。トークンをまだお持ちでない場合は、RHACS Configuration Management Cloud Service ポータルでトークンを生成できます。
4. **Save** をクリックして認証情報を保存し、Add Credential ウィザードを閉じます。

3.6.3. ソースおよび認証情報について

スキャンを実行するには、ソースと認証情報の 2 つの基本的な構造のデータを設定する必要があります。スキャン中に検査するソースのタイプによって、ソースと認証情報の両方の設定に必要なデータのタイプが決まります。

ソース には、スキャン時に検査される単一のアセットまたは複数のアセットが含まれます。以下の 4 種類のソースを設定できます。

ネットワークソース
: 1 つ以上の物理マシン、仮想マシン、またはコンテナー。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表現可能。

vCenter ソース
: IT インフラストラクチャーのすべてまたは一部を管理する vCenter Server システム管理ソリューション。

Satellite ソース
: IT インフラストラクチャーのすべてまたは一部を管理する Satellite システム管理ソリューション。

Red Hat OpenShift ソース
: Red Hat OpenShift Container Platform ノードおよびワークロードのすべてまたは一部を管理する Red Hat OpenShift Container Platform クラスター。

Ansible ソース
: Ansible ノードとワークロードを管理する Ansible 管理ソリューション。

Red Hat Advanced Cluster Security for Kubernetes ソース
: Kubernetes 環境をセキュリティー保護する RHACS セキュリティープラットフォームソリューション。

ネットワークソースを使用している場合は、単一のソース内でグループ化する必要がある個々のアセットの数を決定します。現在、ネットワークソースに対してのみ、複数のアセットをソースに追加できます。次のリストには、ソースを追加するときに考慮する必要があるその他の要因がいくつか含まれています。

- アセットが開発、テスト、または本番環境の一部であるかどうか、およびコンピューティング能力の要求と同様の懸念がそれらのアセットの考慮事項であるかどうか。
- インストールされたソフトウェアへの頻繁な変更などの内部ビジネス慣習のために、特定のエンティティーまたはエンティティーのグループをより頻繁にスキャンするかどうか。

認証情報 は、ソースに含まれるアセットのすべてまたは一部でスキャンを実行する権限を持つユーザーのユーザー名やパスワード、SSH キーなどのデータが含まれます。ソースと同様に、認証情報はネットワーク、vCenter、Satellite、OpenShift、Ansible、または RHACS タイプとして設定されます。通常、ネットワークソースには、幅広い IP 範囲内の全アセットにアクセスするために多くの認証情報が必要になることが想定されるため、複数のネットワーク認証情報が必要になる場合があります。逆に、vCenter または Satellite ソースは、通常、必要に応じて単一の vCenter または Satellite 認証情報を使用して特定のシステム管理ソリューションサーバーにアクセスします。また、OpenShift、Ansible、または RHACS ソースは、単一のクラスターにアクセスするために単一の認証情報を使用します。

Sources ビューから新しいソースを追加でき、Credentials ビューから新しい認証情報を追加できます。ソースの作成中に、新しい認証情報を追加したり、既存の認証情報を選択したりすることもできます。認証情報をソースに直接関連付けるのは、ソースの作成時です。ソースと認証情報には一致するタイプが必要なため、ソースの作成時に追加する認証情報はソースと同じタイプを共有します。さらに、ソースの作成時に既存の認証情報を使用する場合は、利用可能な認証情報のリストに同じタイプの認証情報のみが含まれます。たとえば、ネットワークソースの作成時に利用できるのは、ネットワーク認証情報のみです。

3.6.4. Red Hat Advanced Cluster Security for Kubernetes 認証

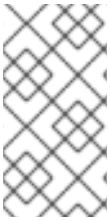
Red Hat Advanced Cluster Security for Kubernetes (RHACS) スキャンの場合、RHACS API への接続性とアクセスは、TLS (Transport Layer Security) で暗号化された API トークンを使用したベアラートークン認証から導出されます。デフォルトでは、RHACS スキャンは TLS プロトコルを介した証明書の検証とセキュアな通信を使用して実行されます。ソースの作成時に、証明書の検証とセキュアな通信に使用するいくつかの異なる SSL (Secure Sockets Layer) および TLS プロトコルから選択できます。

スキャン中に RHACS ポータルに接続できるように、証明書検証のレベルの調整が必要な場合があります。たとえば、RHACS インスタンスは、認証局による検証済みの TLS 証明書を使用する場合があります。ソースのスキャン時に証明書を確認できるように、ソースの作成時に TLS 証明書の検証をアップグレードできます。逆に、RHACS インスタンスは自己署名証明書を使用する場合があります。ソースのスキャンで証明書が確認されないように、ソースの作成時に TLS 検証をデフォルトのままにすることができます。このように、自己署名証明書を使用する場合にオプションをデフォルトのままにすることで、スキャンエラーを回避できる可能性があります。

RHACS インスタンスが Web アプリケーションに TSL 通信を使用するように設定されていない場合は、スキャン時のセキュアな通信方法として TSL を無効にする必要がある場合もあります。たとえば、RHACS インスタンスが、ポート 80 で HTTP を使用して Web アプリケーションと通信するように設定されている場合があります。その場合は、ソースの作成時に、そのソースのスキャンに対して TSL 通信を無効にできます。

第4章 スキャンの実行および管理

スキャンする IT インフラストラクチャーの部分のソースおよび認証情報を追加したら、スキャンを作成および実行できます。スキャンの作成時に、単一のソースをスキャンするか、異なるソースタイプから複数のソースを組み合わせることができます。また、デフォルトのインストールプロセスおよび場所にインストールされる製品の標準スキャンを実行するか、標準以外のプロセスまたは場所で製品がインストールされている場合にディープスキャンを実行することもできます。



注記

現在、スキャンで OpenShift、Ansible、または RHACS スキャンを他のタイプのソースと組み合わせることはできません。ただし、単一の OpenShift、Ansible、または RHACS スキャンには同じタイプの複数のソースを含めることができます。その場合、各ソースは単一のクラスターのみに関連付けられます。

スキャンの作成後、そのスキャンを複数回実行できます。スキャンの各インスタンスはスキャンジョブとして保存されます。

詳細情報

製品にディープスキャンを使用しない標準スキャンを実行する方法は、以下の情報を参照してください。

- 標準スキャンの実行および管理

ディープスキャン (標準以外のプロセスまたは非標準の場所にインストールされている可能性のある製品を検出できるスキャン) の実行の詳細は、次の情報を参照してください。

- ディープスキャンの実行および管理

4.1. 標準スキャンの実行および管理

スキャンする IT インフラストラクチャーの部分のソースと認証情報を追加したら、スキャンの実行を開始できます。ほとんどの場合は、標準スキャンを実行して、Red Hat 製品に関するレポートに必要な環境および製品データを探すことができます。

詳細情報

標準スキャンを実行して、標準の場所に製品を見つけます。詳細は、以下の情報を参照してください。

- 標準スキャンの実行

スキャンの実行を開始すると、スキャンの管理に使用できるタスクがいくつかあります。これらのタスクには、新しいスキャンジョブを実行して、スキャンのデータを更新し、一時停止、再開、およびキャンセルによるアクティブなスキャンを管理することが含まれます。スキャンが終了したら、スキャンを削除できます。詳細は、以下の情報を参照してください。

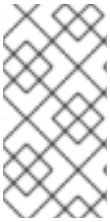
- 新しいスキャンジョブの実行
- スキャンの一時停止、再開、およびキャンセル
- スキャンの削除

スキャンとスキャンジョブの仕組み、具体的には Discovery によるスキャンジョブの処理方法、スキャンジョブがライフサイクル中に移動する状態などの詳細は、次の情報を参照してください。

- スキャンおよびスキャンジョブについて
- ジョブ処理のスキャン
- ジョブライフサイクルのスキャン

4.1.1. 標準スキャンの実行

Sources ビューから新しいスキャンを実行できます。1 つのソースのスキャンを実行するか、複数のソースを選択して 1 つのスキャンに統合できます。Sources ビューを使用してスキャンを実行するたびに、新しいスキャンとして保存するように求められます。



注記

現在、スキャンで OpenShift、Ansible、または RHACS スキャンを他のタイプのソースと組み合わせることはできません。ただし、単一の OpenShift、Ansible、または RHACS スキャンには同じタイプの複数のソースを含めることができます。その場合、各ソースは単一のクラスターのみに関連付けられます。

スキャンを初めて実行した後、スキャンはスキャンビューに保存されます。その表示から、再度スキャンを実行してデータを更新できます。Scans ビューからスキャンを実行するたびに、スキャンの新しいスキャンジョブとして保存されます。

前提条件

- スキャンを実行するには、最初にスキャンするソースと、そのソースにアクセスするための認証情報を追加している。

手順

1. Sources ビューで、1 つ以上のソースを選択します。異なるタイプのソースを選択して 1 つのスキャンに統合できます。
2. 選択したソースに適した **Scan** ボタンをクリックします。
   - 単一ソースの場合は、そのソースの行にある **Scan** をクリックします。ソースのチェックボックスの選択は任意です。
   - 複数のソースを選択した場合は、ツールバーの **Scan** をクリックします。

   スキャンウィザードが開きます。
3. **Name** フィールドに、スキャンの説明的な名前を入力します。
4. 最大同時スキャンのデフォルト数を変更する場合は、**Maximum concurrent scans** フィールドに新しい値を設定します。この値は、スキャン中に並行してスキャンされる物理マシンまたは仮想マシンの最大数です。
5. デフォルトのスキャンプロセスを使用するには、**Deep scan for these products**チェックボックスがデフォルトのオフのままになるようにします。
6. スキャンプロセスを開始するには、**Scan** をクリックします。

検証手順

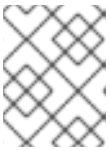
スキャンプロセスが開始すると、Sources ビューに通知が表示されます。実行中のスキャンは Scans ビューにも表示され、スキャンの進捗に関するメッセージが表示されます。

4.1.2. 新しいスキャンジョブの実行

スキャンに名前を付け、初めて実行した後、Scans ビューに追加されます。その後、スキャンジョブと呼ばれるスキャンの新しいインスタンスを実行して、スキャン用に収集されるデータを更新できます。

手順

1. Scans ビューで、スキャンの詳細にある **Run Scan** アイコンをクリックします。



注記

スキャンの詳細では、最新のスキャンジョブが正常に完了しないと、このアイコンに **Retry Scan** というラベルが付けられます。

検証手順

スキャンプロセスが開始すると、スキャンの進捗に関するメッセージと共に通知が表示されます。完了したスキャンを表示する場合は、スキャンの詳細を表示して、**Previous** をクリックして展開し、以前のスキャンジョブを表示できます。

4.1.3. スキャンの一時停止、再開、およびキャンセル

スキャンの実行を開始する際に、現在実行中のスキャンジョブを停止する必要がある場合があります。これを行う必要があるさまざまなビジネス上の理由がある可能性があります。たとえば、IT ヘルスモニタリングシステムからのアラートが原因で緊急修正を行う必要がある場合や、優先度の低いスキャンが現在実行している場合により多くの CPU リソースを消費する優先度の高いスキャンを実行しないといけない場合などです。

スキャンジョブを停止するには、一時停止するか、キャンセルします。一時停止したスキャンジョブを再開することはできますが、キャンセルしたスキャンジョブを再開することはできません。

手順

実行中のスキャンジョブを一時停止するには、以下を実行します。

1. Scans ビューで、一時停止するスキャンジョブが含まれるスキャンを見つけます。
2. **Pause Scan** をクリックします。

注記

複数のスキャンが同時に実行している場合は、**Pause Scan** アイコンでスキャンを開始してからしばらく時間がかかる場合があります。

一時停止されているスキャンジョブを再開するには、以下を行います。

1. Scans ビューで、再開するスキャンジョブが含まれるスキャンを見つけます。
2. **Resume Scan** をクリックします。

実行中のスキャンジョブをキャンセルするには、次を行います。

1. Scans ビューで、キャンセルするスキャンジョブが含まれるスキャンを見つけます。
2. **Cancel Scan** をクリックします。

4.1.4. スキャンの削除

スキャンの削除は、スキャンとそのスキャンのすべてのスキャンジョブを削除する元に戻せないアクションです。削除されたスキャンは復元できません。

前提条件

- スキャンを削除するには、まずスキャンを実行して、**Scans** ナビゲーションにスキャンを表示する必要があります。

手順

1. ナビゲーションから **Scans** をクリックします。
2. 削除するスキャンを含む行を見つけます。
3. その行の **Delete** アイコンをクリックします。

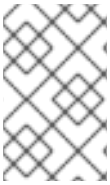
結果

- スキャンは削除されます。

4.1.5. スキャンおよびスキャンジョブについて

ソースおよび認証情報の作成後、スキャンを作成できます。**scan** は、ソースを複製可能な方法で検査またはスキャンできるユニットにグループ化するオブジェクトです。保存したスキャンを実行するたびに、そのインスタンスは **スキャンジョブ** として保存されます。スキャンジョブの出力は **レポート** で、そのソースに含まれるすべての IT リソースに対して収集されたファクトのコレクションです。

スキャンには、少なくとも 1 つのソースと、ソースの作成時にそのソースに関連付けられた認証情報が含まれます。スキャンジョブが実行すると、提供された認証情報を使用してソースに含まれるアセットに接続し、アセットを検査してレポートに対してこれらのアセットに関するファクトを収集します。異なるタイプのソースの組み合わせを単一のスキャンに追加するなど、複数のソースを単一のスキャンに追加できます。



注記

現在、スキャンで OpenShift ソースを他のタイプのソースと組み合わせることはできません。ただし、1 つの OpenShift スキャンに複数の OpenShift ソースを含めることができます。その場合、各ソースは 1 つのクラスターにのみ関連付けられます。

4.1.6. ジョブ処理のスキャン

スキャンジョブは処理中に 2 つのフェーズまたはタスクを移動します。この 2 つのタスクは接続タスクと検査タスクです。

4.1.6.1. ジョブ接続および検査タスクのスキャン

スキャンジョブ中に実行する最初のタスクはコネクションタスクです。**接続タスク** は、ソースへの接続機能を判断し、定義したソースを検査できるシステム数を見つけます。実行する 2 番目のタスクは、検

査タスクです。**検査タスク** は、定義されたソースの到達可能な各システムからデータを収集し、スキャン結果をレポートに出力するタスクです。

スキャンで複数のソースが含まれるように設定されている場合は、スキャンジョブが実行すると、これらの 2 つのタスクがソースごとに作成されます。まず、すべてのソースの接続タスクを実行してソースへの接続を確立し、検査できるシステムを見つけます。その後、すべてのソースの検査タスクが実行し、ソースに含まれる到達可能なシステムの内容を検証します。

4.1.6.2. これらのタスクの処理方法

スキャンジョブがソースの接続タスクを実行すると、使用されているネットワーク、サーバー、クラスター、またはインスタンスへの接続が試行されます。接続が失敗すると、接続タスクは失敗します。ネットワークスキャンでは、ネットワークに到達できない場合や認証情報が無効な場合、接続タスクが正常なシステムが 0 であることを報告します。ネットワークスキャン用の一部のシステムのみが到達可能であれば、接続タスクは到達可能なシステムで成功を報告し、接続タスクが失敗しません。

Scans ビューで接続タスクのステータスに関する情報を表示できます。スキャンの行には、接続タスクの結果が、最新のスキャンジョブで成功したシステム接続の数として表示されます。以前のスキャンジョブをデプロイメントして、以前のスキャンジョブの接続タスクの結果を表示することもできます。

スキャンジョブがソースの検査タスクを実行すると、コネクションタスクの状態をチェックします。接続タスクで failed 状態が表示される場合や、ゼロ (0) 個の正常接続がある場合、スキャンジョブは failed 状態に移行します。ただし、コネクションタスクは 1 つ以上の接続を報告すると、検査タスクが継続します。その後、スキャンジョブの結果は、各システムの成功データおよび失敗データを表示します。検査タスクが正常なシステムから結果を収集できない場合や、検査タスク中に別の予期しないエラーが発生した場合は、スキャンジョブを failed 状態に切り替えます。

スキャンに複数のソースが含まれていると、各ソースに独自の接続タスクおよび検査タスクがあります。これらのタスクは、他のソースのタスクとは別に処理されます。ソースのいずれかのタスクが失敗すると、スキャンジョブは failed 状態に移行します。スキャンジョブは、すべてのソースに対してすべてのスキャンジョブタスクが正常に完了した場合にのみ完了状態に移行します。

スキャンジョブが正常に完了すると、スキャンジョブのデータがレポートとして生成されます。Scans ビューで、正常なスキャンジョブごとにレポートをダウンロードできます。

4.1.7. ジョブライフサイクルのスキャン

スキャンジョブ、またはスキャンの個別のインスタンスは、ライフサイクル中に複数の状態に変わります。

スキャンを開始すると、スキャンジョブが作成され、スキャンジョブは **created** 状態になります。その後、スキャンジョブは処理のためにキューに置かれ、スキャンジョブが **pending** 状態になります。スキャンジョブは、開始順に順次実行します。

Discovery サーバーがキュー内の特定のスキャンジョブに到達し、そのスキャンジョブの処理が開始すると、そのスキャンジョブは、**pending** 状態から **running** 状態に変わります。スキャンプロセスが正常に完了すると、スキャンジョブは **completed** 状態になり、スキャンジョブがレポートで表示できる結果を生成します。スキャンプロセスで、スキャンが正常に完了しないようにエラーが発生すると、スキャンジョブが停止し、**failed** 状態になります。失敗したスキャンの追加のステータスメッセージには、失敗の原因を特定するのに役立つ情報が含まれています。

スキャンジョブのその他の状態は、スキャンジョブに対して実行したユーザーアクションによって決まります。スキャンジョブが保留中または実行中に一時停止またはキャンセルできます。**paused** 状態のスキャンジョブを再開できます。**canceled** 状態のスキャンジョブを再開できません。

4.2. ディープスキャンの実行および管理

スキャンする IT インフラストラクチャーの部分のソースと認証情報を追加したら、スキャンの実行を開始できます。一部の状況では、Red Hat 製品に関する報告に必要な環境および製品データを見つけるのに、標準スキャンの実行では不十分です。

Discovery はデフォルトで、それらの製品に関連する既知のメタデータを使用して、製品を検索し、フィンガープリントを作成します。ただし、これらの製品を、検索およびフィンガープリントのアルゴリズムの効果を低下させるプロセスまたはインストール場所にインストールした可能性があります。この場合、これらの製品を見つけるには、ディープスキャンを使用する必要があります。

詳細情報

ディープスキャンを実行して、標準以外の場所にある製品を見つけます。詳細は、以下の情報を参照してください。

- ディープスキャンを使用したスキャンの実行

スキャンの実行を開始すると、スキャンの管理に使用できるタスクがいくつかあります。これらのタスクには、新しいスキャンジョブを実行して、スキャンのデータを更新し、一時停止、再開、およびキャンセルによるアクティブなスキャンを管理することが含まれます。スキャンが終了したら、スキャンを削除できます。詳細は、以下の情報を参照してください。

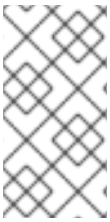
- 新しいスキャンジョブの実行
- スキャンの一時停止、再開、およびキャンセル
- スキャンの削除

スキャンとスキャンジョブの仕組み、具体的には Discovery によるスキャンジョブの処理方法、スキャンジョブがライフサイクル中に移動する状態などの詳細は、次の情報を参照してください。

- スキャンおよびスキャンジョブについて
- ジョブ処理のスキャン
- ジョブライフサイクルのスキャン

4.2.1. ディープスキャンを使用したスキャンの実行

Sources ビューから新しいスキャンを実行できます。1 つのソースのスキャンを実行するか、複数のソースを選択して 1 つのスキャンに統合できます。スキャン設定の一環として、標準以外の場所でディープスキャンプロセスを使用して製品を検索することを選択する場合があります。



注記

現在、スキャンで OpenShift、Ansible、または RHACS スキャンを他のタイプのソースと組み合わせることはできません。ただし、単一の OpenShift、Ansible、または RHACS スキャンには複数の OpenShift、Ansible、または RHACS ソースを含めることができます。その場合、各ソースは単一のクラスターのみに関連付けられます。

詳細なスキャンプロセスでは **find** コマンドを使用するため、スキャンされるシステムに対しては、検索プロセスは CPU リソースを消費する可能性があります。したがって、実稼働システムなどの継続的な可用性を必要とするシステムのディープスキャンを選択する場合は、判断を使用する必要があります。

スキャンを初めて実行した後、スキャンはスキャンビューに保存されます。その表示から、スキャンを再度実行して、データを更新できます。

前提条件

- スキャンを実行するには、最初にスキャンするソースと、そのソースにアクセスするための認証情報を追加している。

手順

1. Sources ビューで、1 つ以上のソースを選択します。異なるタイプのソースを選択して 1 つのスキャンに統合できます。
2. 選択したソースに適した **Scan** ボタンをクリックします。
   - 単一ソースの場合は、そのソースの行にある **Scan** をクリックします。ソースのチェックボックスの選択は任意です。
   - 複数のソースを選択した場合は、ツールバーの **Scan** をクリックします。

   スキャンウィザードが開きます。
3. **Name** フィールドに、スキャンの説明的な名前を入力します。
4. 最大同時スキャンのデフォルト数を変更する場合は、**Maximum concurrent scans** フィールドに新しい値を設定します。この値は、スキャン中に並行してスキャンされる物理マシンまたは仮想マシンの最大数です。
5. 1 つ以上の製品でディープスキャンプロセスを使用するには、以下の情報を指定します。
   - 該当する **Deep scan for these products**チェックボックスを選択します。
   - 必要に応じて、Discovery がスキャンするディレクトリーを入力します。ディープスキャンで使用されるデフォルトのディレクトリーは、/、**/opt**、**/app**、**/home**、および **/usr** ディレクトリーです。
6. スキャンプロセスを開始するには、**Scan** をクリックします。

検証手順

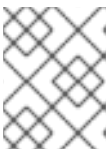
スキャンプロセスが開始すると、Sources ビューに通知が表示されます。実行中のスキャンは Scans ビューにも表示され、スキャンの進捗に関するメッセージが表示されます。

4.2.2. 新しいスキャンジョブの実行

スキャンに名前を付け、初めて実行した後、Scans ビューに追加されます。その後、スキャンジョブと呼ばれるスキャンの新しいインスタンスを実行して、スキャン用に収集されるデータを更新できます。

手順

1. Scans ビューで、スキャンの詳細にある **Run Scan** アイコンをクリックします。



注記

スキャンの詳細では、最新のスキャンジョブが正常に完了しないと、このアイコンに **Retry Scan** というラベルが付けられます。

検証手順

スキャンプロセスが開始すると、スキャンの進捗に関するメッセージと共に通知が表示されます。完了したスキャンを表示する場合は、スキャンの詳細を表示して、**Previous** をクリックして展開し、以前のスキャンジョブを表示できます。

4.2.3. スキャンの一時停止、再開、およびキャンセル

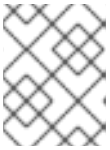
スキャンの実行を開始する際に、現在実行中のスキャンジョブを停止する必要がある場合があります。これを行う必要があるさまざまなビジネス上の理由がある可能性があります。たとえば、IT ヘルスモニタリングシステムからのアラートが原因で緊急修正を行う必要がある場合や、優先度の低いスキャンが現在実行している場合により多くの CPU リソースを消費する優先度の高いスキャンを実行しないといけない場合などです。

スキャンジョブを停止するには、一時停止するか、キャンセルします。一時停止したスキャンジョブを再開することはできますが、キャンセルしたスキャンジョブを再開することはできません。

手順

実行中のスキャンジョブを一時停止するには、以下を実行します。

1. Scans ビューで、一時停止するスキャンジョブが含まれるスキャンを見つけます。
2. **Pause Scan** をクリックします。



注記

複数のスキャンが同時に実行している場合は、**Pause Scan** アイコンでスキャンを開始してからしばらく時間がかかる場合があります。

一時停止されているスキャンジョブを再開するには、以下を行います。

1. Scans ビューで、再開するスキャンジョブが含まれるスキャンを見つけます。
2. **Resume Scan** をクリックします。

実行中のスキャンジョブをキャンセルするには、次を行います。

1. Scans ビューで、キャンセルするスキャンジョブが含まれるスキャンを見つけます。
2. **Cancel Scan** をクリックします。

4.2.4. スキャンの削除

スキャンの削除は、スキャンとそのスキャンのすべてのスキャンジョブを削除する元に戻せないアクションです。削除されたスキャンは復元できません。

前提条件

- スキャンを削除するには、まずスキャンを実行して、**Scans** ナビゲーションにスキャンを表示する必要があります。

手順

1. ナビゲーションから **Scans** をクリックします。

2. 削除するスキャンを含む行を見つけます。

3. その行の **Delete** アイコンをクリックします。

結果

- スキャンは削除されます。

4.2.5. スキャンおよびスキャンジョブについて

ソースおよび認証情報の作成後、スキャンを作成できます。**scan** は、ソースを複製可能な方法で検査またはスキャンできるユニットにグループ化するオブジェクトです。保存したスキャンを実行するたびに、そのインスタンスは **スキャンジョブ** として保存されます。スキャンジョブの出力は **レポート** で、そのソースに含まれるすべての IT リソースに対して収集されたファクトのコレクションです。

スキャンには、少なくとも 1 つのソースと、ソースの作成時にそのソースに関連付けられた認証情報が含まれます。スキャンジョブが実行すると、提供された認証情報を使用してソースに含まれるアセットに接続し、アセットを検査してレポートに対してこれらのアセットに関するファクトを収集します。異なるタイプのソースの組み合わせを単一のスキャンに追加するなど、複数のソースを単一のスキャンに追加できます。

注記

現在、スキャンで OpenShift ソースを他のタイプのソースと組み合わせることはできません。ただし、1 つの OpenShift スキャンに複数の OpenShift ソースを含めることができます。その場合、各ソースは 1 つのクラスターにのみ関連付けられます。

4.2.6. ジョブ処理のスキャン

スキャンジョブは処理中に 2 つのフェーズまたはタスクを移動します。この 2 つのタスクは接続タスクと検査タスクです。

4.2.6.1. ジョブ接続および検査タスクのスキャン

スキャンジョブ中に実行する最初のタスクはコネクションタスクです。**接続タスク** は、ソースへの接続機能を判断し、定義したソースを検査できるシステム数を見つけます。実行する 2 番目のタスクは、検査タスクです。**検査タスク** は、定義されたソースの到達可能な各システムからデータを収集し、スキャン結果をレポートに出力するタスクです。

スキャンで複数のソースが含まれるように設定されている場合は、スキャンジョブが実行すると、これらの 2 つのタスクがソースごとに作成されます。まず、すべてのソースの接続タスクを実行してソースへの接続を確立し、検査できるシステムを見つけます。その後、すべてのソースの検査タスクが実行し、ソースに含まれる到達可能なシステムの内容を検証します。

4.2.6.2. これらのタスクの処理方法

スキャンジョブがソースの接続タスクを実行すると、使用されているネットワーク、サーバー、クラスター、またはインスタンスへの接続が試行されます。接続が失敗すると、接続タスクは失敗します。ネットワークスキャンでは、ネットワークに到達できない場合や認証情報が無効な場合、接続タスクが正常なシステムが 0 であることを報告します。ネットワークスキャン用の一部のシステムのみが到達可能であれば、接続タスクは到達可能なシステムで成功を報告し、接続タスクが失敗しません。

Scans ビューで接続タスクのステータスに関する情報を表示できます。スキャンの行には、接続タスクの結果が、最新のスキャンジョブで成功したシステム接続の数として表示されます。以前のスキャンジョブをデプロイメントして、以前のスキャンジョブの接続タスクの結果を表示することもできます。

スキャンジョブがソースの検査タスクを実行すると、コネクションタスクの状態をチェックします。接続タスクで failed 状態が表示される場合や、ゼロ (0) 個の正常接続がある場合、スキャンジョブは failed 状態に移行します。ただし、コネクションタスクは 1 つ以上の接続を報告すると、検査タスクが継続します。その後、スキャンジョブの結果は、各システムの成功データおよび失敗データを表示します。検査タスクが正常なシステムから結果を収集できない場合や、検査タスク中に別の予期しないエラーが発生した場合は、スキャンジョブを failed 状態に切り替えます。

スキャンに複数のソースが含まれていると、各ソースに独自の接続タスクおよび検査タスクがあります。これらのタスクは、他のソースのタスクとは別に処理されます。ソースのいずれかのタスクが失敗すると、スキャンジョブは failed 状態に移行します。スキャンジョブは、すべてのソースに対してすべてのスキャンジョブタスクが正常に完了した場合にのみ完了状態に移行します。

スキャンジョブが正常に完了すると、スキャンジョブのデータがレポートとして生成されます。Scans ビューで、正常なスキャンジョブごとにレポートをダウンロードできます。

4.2.7. ジョブライフサイクルのスキャン

スキャンジョブ、またはスキャンの個別のインスタンスは、ライフサイクル中に複数の状態に変わります。

スキャンを開始すると、スキャンジョブが作成され、スキャンジョブは **created** 状態になります。その後、スキャンジョブは処理のためにキューに置かれ、スキャンジョブが **pending** 状態になります。スキャンジョブは、開始順に順次実行します。

Discovery サーバーがキュー内の特定のスキャンジョブに到達し、そのスキャンジョブの処理が開始すると、そのスキャンジョブは、**pending** 状態から **running** 状態に変わります。スキャンプロセスが正常に完了すると、スキャンジョブは **completed** 状態になり、スキャンジョブがレポートで表示できる結果を生成します。スキャンプロセスで、スキャンが正常に完了しないようにエラーが発生すると、スキャンジョブが停止し、**failed** 状態になります。失敗したスキャンの追加のステータスメッセージには、失敗の原因を特定するのに役立つ情報が含まれています。

スキャンジョブのその他の状態は、スキャンジョブに対して実行したユーザーアクションによって決まります。スキャンジョブが保留中または実行中に一時停止またはキャンセルできます。**paused** 状態のスキャンジョブを再開できます。**canceled** 状態のスキャンジョブを再開できません。

第5章 レポートのダウンロード

スキャンの実行後、スキャンのレポートをダウンロードして、スキャン中に収集および処理されたデータを表示できます。

詳細情報

レポートのダウンロードに関する詳細は、以下の情報を参照してください。

- レポートのダウンロード

5.1. レポートのダウンロード

スキャンの実行後、スキャンのレポートをダウンロードして、スキャン中に収集および処理されたデータを表示できます。

スキャンのレポートは、コンマ区切り変数 (CSV) 形式と JavaScript Object Notation (JSON) 形式という 2 つの形式で利用できます。また、これらは 2 つのコンテンツタイプで利用できます。スキャンからの raw 出力は、詳細レポートと、デプロイメントレポートとして処理されたコンテンツです。

注記

3 番目のタイプのレポートである Insights レポートを利用できますが、このレポートは、Discovery コマンドラインインターフェイス経由でのみ生成できます。Insights レポートをダウンロードすると、cloud.redhat.com の Hybrid Cloud Console に転送できる **.tar.gz** ファイルが提供されます。このファイルを転送すると、レポートデータを Red Hat Insights インベントリーサービスおよびサブスクリプションサービスで使用できるようになります。

詳細情報

レポートのマージおよびダウンロードの詳細は、以下の情報を参照してください。

- レポートのダウンロード

レポートの作成方法の詳細は、以下の情報を参照してください。この情報には、レポート生成プロセスの経過が含まれます。これらのプロセスは、詳細レポートの生のファクトをフィンガープリントのデータに変更し、次にフィンガープリントのデータからデプロイメントレポートを重複排除してマージしたデータに変更します。この情報には、Discovery レポートの作成に使用されるデータの種類を示す部分的なフィンガープリントの例も含まれます。

- レポートの作成方法
- フィンガープリントの例

5.1.1. レポートのダウンロード

Scans ビューで、1 つ以上のレポートを選択し、それらをダウンロードしてレポートデータを表示できます。

前提条件

スキャンのレポートをダウンロードする場合は、スキャンの最新のスキャンジョブが正常に完了している必要があります。

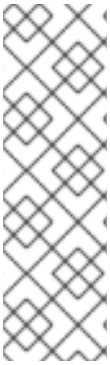
手順

1. Scans ビューで、レポートをダウンロードする必要のあるスキャンの行に移動します。
2. このスキャンの **ダウンロード** をクリックします。

検証手順

ダウンロードしたレポートは、**.tar.gz** ファイルとしてブラウザーをダウンロードできる場所に保存されます (例 : **report_id_224_20190702_173309.tar.gz**)。ファイル形式は **report_id_ID_DATE_TIME.tar.gz** です。**ID** はサーバーが割り当てた一意のレポート ID に、**DATE** は **yyyymmdd** 形式の日付に、**TIME** は 24時間形式をもとにした **hhmmss** 形式の時間に置き換えます。日付および時間のデータは、クライアントをサーバー API と共に実行しているブラウザーとの対話によって決まります。

レポートを表示するには、**.tar.gz** ファイルを **report_id_ID** ディレクトリーに展開します。展開したレポートバンドルには 4 つのレポートファイルが含まれます (CSV 形式および JSON 形式の 2 つの詳細レポートと、CSV 形式および JSON 形式の 2 つのデプロイメントレポートが含まれます)。



注記

これらのレポートの出力を表示して、独自の内部プロセスに使用することはできますが、Discovery ドキュメントには、レポートの結果を解釈するのに役立つ情報が含まれていません。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、レポートを理解するためのサポートは提供しません。レポートとその形式は、Red Hat Subscription Education and Awareness Program (SEAP) チームが顧客とのエンゲージメントに使用したり、さまざまな Hybrid Cloud Console サービスへのデータ提供など、他の Red Hat 内部プロセスで使用するように設計されています。

5.1.2. レポートの作成方法

スキャンプロセスは、IT インフラストラクチャーでシステムを検出し、それらのシステムの性質および内容に関する情報を収集し、各システムの調査中に収集した情報からレポートを作成するために使用されます。

システム は、SSH 接続、vCenter Server データ、Satellite Server API、または Red Hat OpenShift クラスター API を使用して、検査タスクにより問い合わせることができるエンティティーです。したがって、システムは物理マシンや仮想マシンなどのマシンである場合もあれば、コンテナーやクラスターなどの別のタイプのエンティティーである場合もあります。

5.1.2.1. ファクトとフィンガープリント

スキャン中、各ソースに含まれるシステムごとにファクトのコレクションが収集されます。**ファクト** とは、オペレーティングシステムのバージョン、CP U コアの数、Red Hat 製品の消費されたエンタイトルメントなど、システムに関する単一のデータです。

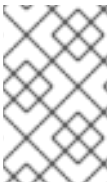
ファクトは、各システム用に要約された一連のデータ (フィンガープリントとして知られているデータ) を作成するために処理されます。**フィンガープリント** とは、アーキテクチャー、オペレーティングシステム、そのシステムにインストールされているさまざまな製品とそのバージョン、そのシステムで使用されるエンタイトルメントなど、一意のシステムとその特性を特定する一連のファクトです。

スキャンジョブを実行すると、フィンガープリントデータが生成されますが、データは 1 種類のレポートのみを作成するために使用されます。詳細レポートを要求すると、フィンガープリントがないスキャンの未加工のファクトが表示されます。デプロイメントレポートを要求すると、重複排除、マージ、処理後のプロセスからの結果を含むフィンガープリントデータを受け取ります。これらのプロセスには、

未加工のファクトからインストールされた製品とバージョンの特定、使用されたエンタイトルメントの検索、さまざまなソースからの製品の重複インスタンスの検索とマージ、デフォルト以外の場所にインストールされた製品の検索などが含まれます。

5.1.2.2. システムの重複排除とマージ

単一のシステムは、スキャン中に複数のソースを確認できます。たとえば、vCenter Server 上の仮想マシンは、Satellite にも管理される Red Hat Enterprise Linux オペレーティングシステムのインストールを実行できます。各タイプの source、vCenter、satellite、および network が含まれるスキャンを作成すると、その 1 つのシステムは、スキャン時に 3 つのソースすべてにより報告されます。



注記

現在、スキャンで OpenShift または Ansible ソースを他のタイプのソースと組み合わせることはできないため、重複排除およびマージプロセスは OpenShift または Ansible スキャンには適用されません。

この問題を解決して正確なフィンガープリントを作成するには、スキャンから未処理のシステムのファクトをフィンガーエンジンに提供します。フィンガープリントエンジンは、重複排除とマージプロセスを使用して、複数のソースにあるシステムのデータを照合し、マージします。

システムの重複排除プロセスは、システムに関する特定のファクトを使用して、重複システムを特定します。このプロセスは、これらのファクトを使用して複数のフェーズに移動し、連続して詳細なデータセットで重複したシステムを組み合わせます。

- ネットワークソースのすべてのシステムは、1 つのネットワークシステムセットに統合されます。**subscription_manager_id** ファクトまたは **bios_uuid** ファクトに同じ値があると、システムが重複しているとみなされます。
- vCenter ソースからのすべてのシステムは、1 つの vCenter システムセットに統合されます。**vm_uuid** ファクトに同じ値があると、システムが重複していると見なされます。
- satellite ソースのすべてのシステムは、1 つのサテライトシステムセットに統合されます。**subscription_manager_id** ファクトに同じ値があると、システムが重複していると見なされます。
- ネットワークシステムセットは、単一の network-satellite システムセットを形成するために設定された Satellite システムとマージされます。**subscription_manager** に同じ値がある場合や、**mac_addresses** ファクトで MAC アドレスの値と一致する場合は、システムが重複していると見なされます。
- network-satellite システムセットは、完全なシステムセットを形成する vCenter システムとマージされます。**mac_addresses** ファクトで MAC アドレス値が一致する場合や、**vm_uuid** ファクトの vCenter 値が **bios_uuid** ファクトのネットワーク値と一致する場合は、システムが重複していると見なされます。

5.1.2.2.1. システムのマージ

重複排除プロセスで 2 つのシステムが重複していると判断した後、次の手順では、2 つのシステムのマージを実行します。マージされたシステムには、各ソースからのシステムファクトがまとめられています。2 つのシステムで表示されるファクトがマージされると、マージプロセスでは、以下の順序で、そのファクトを上から下にマージします。

1. network ソースファクト

2. satellite ソースファクト

3. vCenter ソースファクト

システムフィンガープリントには、そのシステムに対する各ファクトの元のソースを取得する **metadata** ディクショナリーが含まれています。

5.1.2.3. システム後処理

重複排除とマージが完了したら、派生したシステムファクトを作成する処理後のフェーズがあります。**派生したシステムファクト** は、複数のシステムファクトの評価から生成されたファクトです。派生したシステムファクトの大半は、特定の製品とそのバージョンの存在など、製品識別データに関連します。

以下の例は、派生したシステムファクト **system_creation_date** の作成方法を示しています。

system_creation_date ファクトは、実際のシステム作成時間が含まれる派生システムファクトです。このファクトの値は、以下のファクトの評価によって決まります。各ファクトの値は、次の優先順位で検査されます。優先順位は、実際のシステム作成時間との一致の精度により決まります。**system_creation_date** ファクトの値を判断するために、空でない最大値が使用されます。

1. **date_machine_id**

2. **registration_time**

3. **date_anaconda_log**

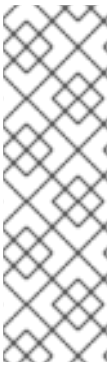
4. **date_filesystem_create**

5. **date_yum_history**

5.1.2.4. レポートの作成

レポートデータの処理が完了すると、レポート作成プロセスは、JSON (JavaScript Object Notation) およびコンマ区切り変数 (CSV) の 2 つの異なる形式でレポートを作成します。各フォーマットの **詳細** レポートには、未処理で未加工なファクトが含まれ、各形式の **デプロイメント** レポートには、フィンガープリント、重複排除、マージ、および処理後のプロセスで未処理のファクトが渡された後の出力が含まれます。

このレポート形式は、Red Hat Subscription Education and Awareness Program (SEAP) チームが顧客とのエンゲージメントやその他の Red Hat 社内プロセスで使用するように設計されています。



注記

これらのレポートの出力を表示して、独自の内部プロセスに使用することはできますが、Discovery ドキュメントには、レポートの結果を解釈するのに役立つ情報が含まれていません。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、レポートを理解するためのサポートは提供しません。レポートとその形式は、Red Hat Subscription Education and Awareness Program (SEAP) チームが顧客とのエンゲージメントに使用したり、さまざまな Hybrid Cloud Console サービスへのデータ提供など、他の Red Hat 内部プロセスで使用するように設計されています。

5.1.2.5. フィンガープリントの例

フィンガープリントは、システム上の製品、エンタイトルメント、ソース、メタデータに加えて、1 つ

のシステムに関するファクトのセットで設定されています。以下の例は、フィンガープリントデータを示しています。Red Hat 製品がほとんどインストールされていない場合でも、1 台システムのフィンガープリント行は多くなる可能性があります。したがって、この例では部分的なフィンガープリントのみが使用されます。

例


```
{
    "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"
        }
    ]
}
```

フィンガープリントの最初の数行は、オペレーティングシステムや CPU に関するファクトを含む、システムに関するファクトを示しています。この例では、**os_release** ファクトで、インストールされているオペレーティングシステムとリリースが **Red Hat Enterprise Linux Atomic Host 7.4** として説明されています。

次に、フィンガープリントは、**products** セクションにインストールされている製品をリスト表示します。製品には、name、version、presence、および metadata フィールドがあります。JBoss EAP セクションでは、**presence** フィールドの値が **absent** と表示されるため、この例のシステムには Red Hat JBoss Enterprise Application Platform がインストールされていません。

また、フィンガープリントには、**entitlements** セクションで、そのシステムの消費済みエンタイトルメントも表示されます。リストの各エンタイトルメントには、そのファクトの元のソースを記述する名前、ID、メタデータがあります。フィンガープリントのサンプルでは、システムに **Satellite Tools 6.3** のエンタイトルメントがあります。

products セクションおよび **entitlements** セクションにあるメタデータフィールドに加えて、フィンガープリントには、システムファクトメタデータに使用される **metadata** セクションが含まれます。システムファクトごとに、フィンガープリントの **metadata** セクションに対応するエントリーがあります。そのエントリーは、そのシステムファクトの元のソースを識別します。この例では、Satellite Server で **os_release** ファクトがサテライトソースのスキャンで検出されました。

最後に、フィンガープリントは、**sources** セクションにこのシステムを含むソースをリスト表示します。システムは、複数のソースに含めることができます。たとえば、スキャンに network ソースと Satellite ソースの両方が含まれていると、スキャンの両方の部分で 1 台のシステムが見つかる可能性があります。

第6章 HYBRID CLOUD CONSOLE へのレポートの送信

スキャンを実行した後、そのスキャンのレポートを cloud.redhat.com の Hybrid Cloud Console に送信できます。生成して送信するレポートは、詳細レポートまたはデプロイメントレポートではなく、**Insights レポート** と呼ばれる 3 番目のタイプのレポートです。このタイプのレポートは、特に Hybrid Cloud Console サービスによる取り込み用にフォーマットされています。

Insights レポートを Hybrid Cloud Console に送信すると、レポートデータは、ホストベースのインベントリーデータを表示する Red Hat Insights のインベントリーサービスや、サブスクリプションの使用状況データを表示するサブスクリプションサービスなど、Hybrid Cloud Console サービスによって取り込まれ、使用されます。

詳細情報

Insights レポートの操作方法の詳細は、次の情報を参照してください。

- Insights レポートのダウンロードと Hybrid Cloud Console への送信

Insights レポートの概念の詳細は、次の情報を参照してください。

- Insights レポートとは何ですか?

6.1. INSIGHTS レポートのダウンロードと HYBRID CLOUD CONSOLE への送信

レポートデータを Red Hat Insights インベントリーサービスやサブスクリプションサービスなどの Hybrid Cloud Console サービスに提供する必要がある場合は、Insights レポートをダウンロードして送信します。

このタイプのレポートは、詳細レポートやデプロイメントレポートとは異なります。**Insights レポート** は、デプロイメントレポートに似たデータを含む Discovery レポートですが、その内容と形式は特に、Hybrid Cloud Console サービスによって取り込まれて使用されるように設計されています。さらに、Insights レポートは、Discovery グラフィカルユーザーインターフェイスから作成することはできません。Discovery コマンドラインインターフェイスを使用して作成する必要があります。

前提条件

Insights レポートをダウンロードして送信するには、次の要件を満たす必要があります。

- そのスキャンの最新のスキャンジョブが正常に完了している必要があります。
- Discovery コマンドラインインターフェイスから以下の手順を実行できるように、コマンドラインインターフェイスは Discovery サーバーと同じシステムにインストールする必要があります。グラフィカルユーザーインターフェイスから Insights レポートをダウンロードして送信することはできません。

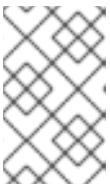
手順

1. コマンドラインインターフェイスにログインします。ここで、**server_administrator_username** は Discovery サーバー管理者のユーザー名で、**server_administrator_password** はサーバー管理者のパスワードです。

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

2. Insights レポートの作成に使用するスキャンジョブの **report_identifier** (レポート ID) の値を見つけます。次のコマンドは、作成されたすべてのスキャンオブジェクトの概要の詳細を返します。

```
$ dsc scan list
```



注記

使用するスキャンの名前はわかっているが、**report_identifier** の値がわからない場合は、**qpc scan show --name scan_name** コマンドを使用して、そのスキャンのみのスキャンジョブを表示することもできます。

3. 特定した **report_identifier** 値を使用して、スキャンジョブの分析情報レポートをダウンロードします。次のコマンド例では、ダウンロードしたレポートに割り当てられたファイル名は **report.tar.gz** ですが、必要に応じてこのファイル名を変更できます。

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

4. Hybrid Cloud Console へのログインに使用する認証情報 (通常は Red Hat Customer Portal アカウント) をコマンドラインインターフェイスの設定に追加します。この手順は、次の手順でこれらの認証情報を使用してインサイトレポートを Hybrid Cloud Console に送信できるようにするために必要です。

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

5. **publish** サブコマンドを使用して、Insights レポートデータを Hybrid Cloud Console、およびレポートを使用できるサービス (インベントリーサービスやサブスクリプションサービスなど) に送信します。

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

注記

Insights レポートの出力を表示することはできますが、Discovery ドキュメントには、Insights レポートの結果を解釈するのに役立つ情報は含まれていません。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、Insights レポートを理解するためのサポートは提供しません。Insights レポートとその形式は、さまざまな Hybrid Cloud Console サービスへのデータの提供など、Red Hat の内部プロセスで使用されるように設計されています。

関連情報

- Discovery コマンドラインインターフェイスのインストールと設定の詳細は、**Discovery のインストールと設定** ガイドを参照してください。

6.2. INSIGHTS レポートとは何ですか?

IT インフラストラクチャーまたは IT インフラストラクチャーの一部でスキャンを実行した後、Discovery を使用して、スキャンからのデータを使用して分析情報レポートを作成できます。Insights レポートは、ホストベースのインベントリーデータを表示する Red Hat Insights のインベントリーサービスや、サブスクリプションの使用状況データを表示するサブスクリプションサービスなど、Hybrid Cloud Console サービスに送信することを目的とした特殊なレポートです。

Discovery は、(オンラインとオフラインの両方の) IT インフラストラクチャーの全部分のスキャンとレポート作成に役立ちますが、IT インフラストラクチャーの一部がオフラインの場合やエアギャップがある場合に Insights レポートを Hybrid Cloud Console サービスに送信する機能は特に役立ちます。Discovery を使用してネットワークのこれらの部分に関するデータを収集して、お使いのネットワーク全体に対する見解が、より包括的で精選されたものになります。Insights レポートのデータを、Hybrid Cloud Console をサポートするツールからの他のデータコレクションと組み合わせると、Hybrid Cloud Console という 1 つの場所で、統合されたインベントリーとサブスクリプションの使用状況の全体像を確認できます。

6.2.1. レポートの頻度

オフラインのシステムやエアギャップのあるシステムはすべて定期的にスキャンし、Insights レポートを通じてレポートして、正確なデータが Hybrid Cloud Console に到達していることを確認する必要があります。Insights レポートを毎週送信することが現在の推奨事項です。1 週間ごとに行う場合には、マイルストーンとして、サブスクリプションサービスでのサブスクリプションの使用状況を効果的に監視するには十分です。

6.2.2. システムの重複回避

Insights レポートで提供するデータの種類によっては、データのマスキングがそのレポートの品質に影響を与える可能性があります。特に、レポート作成の重複排除およびマージプロセスで顕著です。

たとえば、Insights レポートに IT インフラストラクチャーのオンライン部分とオフライン部分の両方のデータが含まれており、そのレポート内のデータをマスクしている場合、Red Hat Satellite や Red Hat Insights などの他の方法でもレポートされている接続システムが重複します。したがって、Red Hat Insights、Satellite、Red Hat Subscription Management、または同様のツールを介して直接報告されているシステムがすでにある場合は、ホスト名、IP アドレス、および Insights レポートを生成するときにシステムを区別するのに役立つこのようなファクトをマスキングしないようにする必要があります。

一般的に、IT インフラストラクチャーのオフライン部分のみを対象にするスキャン、または完全にオフラインの顧客側のスキャンでは、一貫したハッシュ値が使用されている場合にマスキングが任意の手順となっています。ただし、マスキングは推奨しません。マスキングは、個々のシステムを区別するために使用される情報のタイプを排除するため、マスキングを使用すると、Red Hat Insights およびサブスクリプションサービスなどの他の Hybrid Cloud Console ツールによって提供される利点の大部分を得ることができなくなります。