Red Hat CloudForms 4.2

プロバイダーの管理

インフラストラクチャー、クラウド、コンテナープロバイダーの管理

Red Hat CloudForms Documentation Team

Red Hat CloudForms 4.2 プロバイダーの管理

インフラストラクチャー、クラウド、コンテナープロバイダーの管理

Red Hat CloudForms Documentation Team
cloudforms-docs@redhat.com

概要

本ガイドでは、Red Hat CloudForms におけるインフラストラクチャー、クラウド、コンテナープロバイダーの管理について説明します。 本ガイドを改善するためのご意見やご提案をお寄せいただく場合、またはエラーを発見された場合には、http://bugzilla.redhat.com で Red Hat CloudForms Management Engine の Documentation コンポーネントを指定して、Bugzilla レポートを提出してください。セクション番号、ガイド名、CloudForms のバージョンなど具体的な情報を記載していただけると、より迅速に対応することができます。

目次

第1章 インフラストラクチャープロバイダー

Red Hat CloudForms において、インフラストラクチャープロバイダーとは、 Red Hat CloudForms アプライアンスを追加して環境内のリソースの管理やそれらのリソースとの対話を行うことができる仮想インフラストラクチャー環境のことを指します。本章では、Red Hat CloudForms に追加可能なインフラストラクチャープロバイダーの異なるタイプとそれらの管理方法について説明します。

Web インターフェースは、仮想サムネイルでプロバイダーを示します。各サムネイルは、デフォルトで 4 分割表示され、各プロバイダーの基本情報を確認することができます。

1. ホスト数
2. 管理システムソフトウェア
3. 現在未使用
4. 認証ステータス

アイコン	説明
	検証済み: 有効な認証情報が追加済みです。
	無効: 認証情報が無効です。
	不明: 認証ステータスが不明か、認証情報が入力されていません。

1.1. インフラストラクチャープロバイダーの検出

プロバイダーを個別に追加する代わりに、指定したサブネット範囲内の全インフラストラクチャープロバイダーを検出することも可能です。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。

2. (**構成**)をクリックして、 (**インフラストラクチャープロバイダーの検出**) を選択します。

3. 検出するプロバイダーのタイプを選択します。

4. **開始アドレス** で始まり、**終了アドレス** で終わる IP アドレスの **サブネット範囲** を入力します。各オクテットを完了するとカーソルが自動的に進みます。

5. **開始** をクリックします。

アプライアンスは指定したサブネット範囲内で全インフラストラクチャープロバイダーを検索し、ユーザーインターフェースに追加します。ただし、検出機能を使用して追加されたプロバイダーを管理できるようにするには、各プロバイダーを編集して、認証情報を指定する必要があります。

1.2. RED HAT VIRTUALIZATION MANAGER プロバイダー

Red Hat Virtualization Manager プロバイダーを使用するには、アプライアンスに追加して、そのホストを認証します。

1.2.1. Red Hat Virtualization Manager プロバイダーの追加

初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、Red Hat Virtualization Manager プロバイダーをアプライアンスに追加します。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。

2. (**構成**) をクリックして (**新規インフラストラクチャープロバイダーの追加**) を選択します。

3. 追加するプロバイダーの **名前** を入力します。この **名前** により、コンソールでデバイスがラベル付けされます。

4. **タイプ** の一覧から **Red Hat Virtualization Manager** を選択します。

5. プロバイダーの **ホスト名または IP アドレス (IPv4 または IPv6)** を入力します。

重要

ホスト名 には、一意の完全修飾ドメイン名を使用する必要があります。

6. プロバイダーがアクセスに標準以外のポートを使用する場合には、**API ポート** を入力します。

7. プロバイダー用に適切な **ゾーン** を選択します。デフォルトでは、ゾーンは **default** に設定されます。

8. **認証情報** セクションの **Default** には、Red Hat Virtualization Manager の管理ユーザーに必要なログイン認証情報を入力します。

   - **ユーザー名** フィールドに、**`admin@internal`** というユーザー名を入力します。
   - **パスワード** フィールドに、パスワードを入力します。

- **パスワードの確認** フィールドでパスワードを確認します。
- **検証** をクリックして Red Hat CloudForms が Red Hat Virtualization Manager に接続できることを確認します。

9. **C & U データベース** タブで、Red Hat Enterprise Virtualization Data Warehouseデータベースの Red Hat CloudForms ユーザー用のログイン認証情報を指定します。

> **重要**
>
> 容量と使用状況のデータを収集するには、設定メニューの **構成** → **サーバー** → **サーバー制御** で容量と使用状況のサーバーロールを有効にする必要があります。**『Deployment Planning Guide』**の「Assigning the Capacity and Utilization Server Roles」のセクションを参照してください。

> **重要**
>
> Red Hat Enterprise Virtualization 環境の容量と使用状況のデータを収集するには、Data Warehouse および Reports のコンポーネントをその環境にインストールして、Data Warehouse データベースに Red Hat CloudForms ユーザーを作成する必要があります。
>
> Data Warehouse および Reports のコンポーネントを Red Hat Virtualization 環境にインストールする方法については、『Red Hat Virtualization インストールガイド』 を参照してください。
>
> Data Warehouse データベースに Red Hat CloudForms ユーザーを作成する方法については、**『Deployment Planning Guide』**の「Data Collection for Red Hat Enterprise Virtualization 3.3 and 3.4」のセクションを参照してください。

- **ユーザー名** のフィールドに、データベースユーザーの名前を入力します。
- **パスワード** のフィールドに、データベースユーザーのパスワードを入力します。
- **パスワードの確認** のフィールドにデータベースユーザーのパスワードを再度入力して確認します。
- **検証** をクリックして、Red Hat CloudForms がデータベースに接続できることを確認します。

10. **保存** をクリックします。

1.2.2. Red Hat Enterprise Virtualization のホストの認証

Red Hat Enterprise Virtualization インフラストラクチャーを追加した後には、そのホストを認証して、完全に機能するようにする必要があります。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. プロバイダーをクリックして概要の画面を表示します。
3. 概要の画面で、**リレーションシップ** 情報のボックス内で **ホスト** をクリックして、そのプロバイダーのホストを表示します。

4. 認証するホストを選択します。**すべてをチェック** オプションを使用すると、全ホストを選択することができます。

5. (**構成**) をクリックします。

6. (**この項目の編集**) をクリックします。

7. **認証情報** のセクションで、必要に応じて以下の認証情報を入力します。

    a. **デフォルト**: このフィールドは、必須です。ユーザーは root または管理者などの権限がある必要があります。

    b. **リモートログイン**: このフィールドの認証情報は、SSH ログインが **デフォルト** のアカウントで無効化されている場合に必要です。

    c. **Web サービス**: このタブは、Red Hat Virtualization Manager の Web サービスへのアクセスに使用します。

    d. **IPMI**: このタブは、IPMI へのアクセスに使用します。

8. **検証** をクリックします。

9. 複数のホストを編集する場合:

    a. **検証対象のホストを選択** の一覧からホストを 1 つ選択します。

    b. 必要な場合には、**リモートログイン**、**Web サービス**、および **IPMI** の認証情報をそれぞれのタブで入力します。**検証** をクリックします。

    c. これらの認証情報を検証する対象のホストを選択します。

10. **追加** をクリックします。

1.3. OPENSTACK インフラストラクチャープロバイダー

OpenStack インフラストラクチャープロバイダーをアプライアンスに追加して有効化します。

1.3.1. OpenStack インフラストラクチャープロバイダーの追加

初期インストールと Red Hat CloudForms 環境の作成が完了した後に、OpenStack インフラストラクチャープロバイダーをアプライアンスに追加します。Red Hat CloudForms は OpenStack `admin` テナントの運用をサポートしています。OpenStack インフラストラクチャープロバイダーの `admin` ユーザーは OpenStack `admin` テナントのデフォルト管理者なので、Red Hat CloudForms で OpenStack インフラストラクチャープロバイダーを作成する際にはこのアカウントを選択してください。`admin` の認証情報を使用する場合には、Red Hat CloudForms のユーザーは `admin` テナント内にプロビジョニングを行い、`admin` テナントに関連付けられたイメージ、ネットワーク、インスタンスを確認することができます。

注記

Red Hat CloudForms でイベントのモニタリングに Telemetry サービスを使用するか、Advanced Message Queueing Protocol (AMQP) を使用するかを設定することができます。Telemetry を選択する場合には、最初に **ceilometer** サービスをアンダークラウド上でイベントを保管するように設定する必要があります。手順については、「アンダークラウドでイベントを保管するための設定」を参照してください。

詳しい情報は、Red Hat OpenStack Platform **『アーキテクチャーガイド』**の「OpenStack Telemetry (ceilometer)」のセクションを参照してください。

1. **コンピュート → インフラストラクチャー → プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規インフラストラクチャープロバイダーの追加**) を選択します。
3. 追加するプロバイダーの **名前** を入力します。この **名前** により、コンソールでデバイスがラベル付けされます。
4. **タイプ** の一覧から **OpenStack Platform Director** を選択します。
5. OpenStack プロバイダーの Keystone サービスの **API バージョン** を一覧から選択します。デフォルトは **`Keystone v2`** です。

   注記

   Keystone API v3 を使用する場合には、ドメインは OpenStack 内のサービスエンティティーの管理の境界を決定するのに使用されます。ドメインにより、ドメイン固有の構成やセキュリティーオプションを設定するなどのさまざまな目的でユーザーをグループ化することができます。詳しい情報は、Red Hat OpenStack Platform **『アーキテクチャーガイド』**の「OpenStack Identity (keystone)」のセクションを参照してください。

6. プロバイダー用に適切な **ゾーン** を選択します。デフォルトでは、ゾーンは **default** に設定されます。

   注記

   詳しい情報は、Red Hat OpenStack Platform **『アーキテクチャーガイド』**の「OpenStack Compute (nova)」のセクションでホストアグリゲートとアベイラビリティーゾーンの定義を参照してください。

7. **デフォルト** タブの **エンドポイント** のセクションで、OpenStack プロバイダーのホストと認証の詳細を設定します。

   a. プロバイダーの **ホスト名または IP アドレス(IPv4 or IPv6)**。プロバイダーがアンダークラウドの場合には、ホスト名を使用します (詳しくは、Red Hat OpenStack Platform **『director のインストールと使用方法』**の「システムのホスト名設定」のセクションを参照してください)。

b. **API ポート** で、OpenStack Keystone サービスに使用するパブリックポートを設定します。デフォルトでは OpenStack はこのサービスにポート 5000 を使用します。

c. OpenStack プロバイダーとの認証に使用する適切な **セキュリティープロトコル** を選択します。

d. **ユーザー名** のフィールドには、アクセス権限のある OpenStack ユーザー名を入力します (例: **admin**)。次に、 対応するパスワードを **パスワード** と **パスワードの確認** のフィールドに入力します。

e. **検証** をクリックして、Red Hat CloudForms が OpenStack プロバイダーに接続できることを確認します。

8. 次に、Red Hat CloudForms が OpenStack プロバイダーからイベントを受信する方法を設定します。**エンドポイント** セクションの **イベント** タブをクリックして設定を開始します。

 - OpenStack プロバイダーの Telemetry サービスを使用するには、**Ceilometer** を選択します。使用する前には、あらかじめプロバイダーを適切に設定しておく必要があります。詳しくは、 「アンダークラウドでイベントを保管するための設定」を参照してください。

 - 代わりに AMQP Messaging バスを使用する場合には、**AMQP** を選択します。その場合には、**ホスト名 (または IPv4 または IPv6 アドレス)** (**エンドポイント** の **イベント** タブ) に AMQP ホストのパブリック IP または修飾ドメイン名を入力します。

   - **API ポート** には、AMQP で使用するパブリックポートを設定します。デフォルトでは、OpenStack はこのホストにポート 5672 を使用します。

   - **ユーザー名** のフィールドには、アクセス権限のある OpenStack ユーザー名を入力します (例: **admin**)。次に、 対応するパスワードを **パスワード** と **パスワードの確認** のフィールドに入力します。

   - **検証** をクリックして認証情報を確認します。

9. OpenStack インフラストラクチャープロバイダーによって管理されている全ホストへの SSH アクセスを設定することも可能です。そのためには、**エンドポイント** セクションの **RSA キーペア** タブをクリックします。

 a. このタブで、アクセス権のあるアカウントの **ユーザー名** を入力します。

 b. **エンドポイント > デフォルト > セキュリティープロトコル** で **SSL** を予め選択していた場合には、**参照** のボタンを使用して秘密鍵を特定し、設定します。

10. インフラストラクチャープロバイダーを設定した後には、**追加** をクリックします。

注記

Red Hat CloudForms では、全 OpenStack サービスの **`adminURL`** エンドポイントが、プライベートではないネットワーク上にある必要があります。したがって、adminURL エンドポイントには、**`192.168.x.x`** 以外の IP アドレスを割り当てます。**`adminURL`** エンドポイントは OpenStack 環境からインベントリーを収集してメトリックをまとめている Red Hat CloudForms Appliance にアクセスできる必要があります。また、すべての Keystone エンドポイントがアクセス可能である必要もあります。アクセスできない場合には、更新が失敗します。

1.3.1.1. アンダークラウドでイベントを保管するための設定

Red Hat CloudForms が Red Hat OpenStack Platform 環境からイベントを受信できるようにするには、その環境内で Compute サービスと Orchestration サービスの **notification_driver** オプションを設定する必要があります。そのためには、アンダークラウドをインストールする前に **undercloud.conf** を編集して、**store_events** と **true** を設定します。関連する詳細情報は、Red Hat OpenStack Platform **『director のインストールと使用方法』の**「アンダークラウドのインストール」および「director の設定」を参照してください。

1.4. VMWARE VCENTER プロバイダー

VMware vCenter プロバイダーを使用するには、アプライアンスに追加して、そのホストを認証します。

1.4.1. VMware vCenter プロバイダーの追加

初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、VMware vCenter プロバイダーをアプライアンスに追加します。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規インフラストラクチャープロバイダーの追加**) を選択します。
3. 追加するプロバイダーの **名前** を入力します。この **名前** により、コンソールでデバイスがラベル付けされます。
4. **タイプ** 一覧から **VMware vCenter** を選択します。
5. プロバイダーの **ホスト名または IP アドレス (IPv4 または IPv6)** を入力します。

   重要

   ホスト名 には、一意の完全修飾ドメイン名を使用する必要があります。

6. プロバイダー用に適切な **ゾーン** を選択します。デフォルトでは、ゾーンは **default** に設定されます。
7. **認証情報** セクションの **Default** には、VMware vCenter の管理ユーザーに必要なログイン認証情報を入力します。
   - **ユーザー名** フィールドにユーザー名を入力します。
   - **パスワード** フィールドに、パスワードを入力します。
   - **パスワードの確認** フィールドでパスワードを確認します。
   - **検証** をクリックして、Red Hat CloudForms が VMware vCenter に接続できることを確認します。
8. **追加** をクリックします。

1.4.2. VMware vCenter ホストの認証

以下の手順では、VMware vCenter ホストの認証方法を説明します。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. プロバイダーをクリックして概要の画面を表示します。
3. 概要の画面で、リレーションシップ 情報のボックス内で **ホスト** をクリックして、そのプロバイダーのホストを表示します。
4. 認証するホストを選択します。**すべてをチェック** オプションを使用すると、全ホストを選択することができます。
5.  (**構成**) をクリックします。
6.  (**選択した項目の編集**) をクリックします。
7. **認証情報** セクションの **Default** には、VMware ESXi のログイン認証情報を入力します。
    - **ユーザー名** フィールドにユーザー名を入力します。
    - **パスワード** フィールドに、パスワードを入力します。
    - **パスワードの確認** フィールドでパスワードを確認します。
    - **検証** をクリックして、Red Hat CloudForms が VMware vCenter ホストに接続できることを確認します。
8. 複数のホストを編集する場合には、**検証対象のホストを選択** の一覧からホストを 1 つ選択します。VMware ESXi にログインするための認証情報を入力して **検証** をクリックします。
9. **保存** をクリックします。

1.4.2.1. ホストの認証情報に管理者以外のアカウントを使用する方法

VMware vCenter インフラストラクチャープロバイダーを追加した後には、そのホストを認証して、完全に機能を有効化する必要があります。管理者の認証情報を使用するか、Red Hat CloudForms 用に作成したロールに割り当てる別のユーザーを作成することができます (ロールの作成方法については、VMware のドキュメントを参照)。管理者以外のユーザーには、以下の権限を有効にする必要があります。

グローバルグループから、以下の項目にチェックを付けます。

- タスクのキャンセル
- 診断
- イベントのログ
- カスタム属性設定の設定
- 設定

以下のグループの全権限セットにチェックを付ける必要があります。

- アラーム
- データストア

- dvPort グループ
- ホスト
- ネットワーク
- リソース
- スケジュール済みのタスク
- タスク
- 仮想マシン
- vSphere Distributed Switch

また、以下のオブジェクトに新規ロールを割り当てる必要があります。

- **データセンター**: データセンターでは、Red Hat CloudForms のユーザー/グループは、少なくともデータセンターレベルでの読み取り専用ロールが必要です (プロパゲーションはなし)。このアクセスがない場合には、リレーションシップを作成することはできません。具体的には、データストアは表示されません。
- **クラスター**: Red Hat CloudForms がアクセスする必要のある各クラスターには、新規ロールを割り当てて、プロパゲーションする必要があります。
- **フォルダー**: Red Hat CloudForms がアクセスする必要のある各フォルダーには、新規ロールを割り当てて、プロパゲーションする必要があります。
- **データストア**: Red Hat CloudForms がアクセスする必要のある各データストアには、新規ロールを割り当てて、プロパゲーションする必要があります。
- **ネットワーク**: Red Hat CloudForms がアクセスする必要のある各 vLAN またはポートグループには、新規ロールを割り当てて、プロパゲーションする必要があります。

1.5. MICROSOFT SCVMM プロバイダー

Microsoft System Center Virtual Machine Manager プロバイダーを使用するには、アプライアンスに追加して、SCVMM サーバーを認証用に設定します。

注記

SCVMM プロバイダーを使用するには、ホストと SCVMM 管理サーバーの間の通信に利用可能なネットワークアダプターが少なくとも 1 つ必要です。SCVMM ホストのプロパティーで、このネットワークアダプターの **Used by Management** にチェックを入れるようにしてください。

1.5.1. Microsoft SCVMM に対する認証

Red Hat CloudForms 環境に Microsoft SCVMM プロバイダーを追加する前には、Microsoft SCVMM サーバー上の HTTP トラフィックをリッスンする WinRM を有効化する必要があります。また、Microsoft SCVMM サーバー上で適切な実行ポリシーを設定して、アプライアンスから PowerShell スクリプトをリモートで実行できるようにする必要もあります。

1. Microsoft SCVMM サーバーへのログイン

2. WinRM を設定できるように有効化します。

```
winrm quickconfig
```

3. 以下のオプションを設定します。

```
winrm set winrm/config/client/auth @{Basic="true"}
winrm set winrm/config/service/auth @{Basic="true"}
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

4. Windows 2012 R2 と PowerShell 4.0 の場合には、以下の構文を使用してこれらのオプションを設定します。

```
winrm set winrm/config/client/auth '@{Basic="true"}'
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

5. Set-ExecutionPolicy コマンドレットを使用して SCVMM サーバーでリモートスクリプト実行を有効化します。

```
Set-ExecutionPolicy RemoteSigned
```

SCVMM リモートスクリプト実行ポリシーについての詳しい情報は、「Set-ExecutionPolicy コマンドレットの使用」を参照してください。

PowerShell がエラーを返した場合には、**evm.log** および **scvmm.log** のファイルで **log_dos_error_results** を検索して情報を確認してください。

1.5.2. Microsoft System Center Virtual Machine Manager プロバイダーの追加

初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、Microsoft System Center Virtual Machine Manager プロバイダーをアプライアンスに追加します。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規インフラストラクチャープロバイダーの追加**) を選択します。
3. 追加するプロバイダーの **名前** を入力します。この **名前** により、コンソールでデバイスがラベル付けされます。
4. **タイプ** の一覧から **Microsoft System Center VMM** を選択します。
5. プロバイダーの **ホスト名または IP アドレス (IPv4 または IPv6)** を入力します。

   重要

   ホスト名 には、一意の完全修飾ドメイン名を使用する必要があります。

6. **セキュリティープロトコル** の一覧から **Kerberos** または **基本 (SSL)** を選択します。

   a. **Kerberos** の場合:

i. Enter the user name and realm in the **ユーザー名** のフィールドでユーザー名とレルムを入力します。

ii. **パスワード** フィールドに、パスワードを入力します。

iii. **パスワードの確認** のフィールドにパスワードを再入力します。

b. **基本 (SSL)** の場合:

i. **ユーザー名** フィールドにユーザー名を入力します。

ii. **パスワード** フィールドに、パスワードを入力します。

iii. **パスワードの確認** のフィールドにパスワードを再入力します。

7. **検証** をクリックして、Red Hat CloudForms が Microsoft System Center Virtual Machine Manager に接続できるかどうかを確認します。

8. **追加** をクリックします。

1.6. プロバイダーの更新

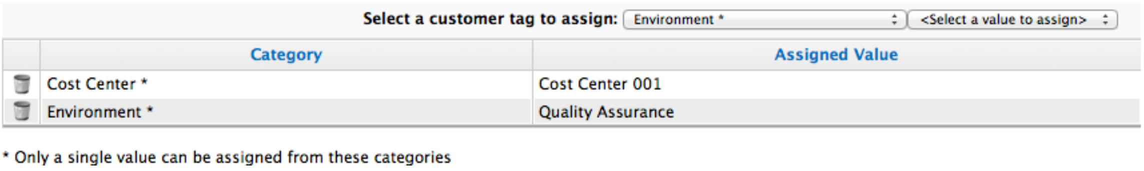
プロバイダーを更新して、関連するその他のリソースを確認します。最初の検出の後に **更新** を使用して、プロバイダーとそのプロバイダーがアクセス可能な仮想マシンについての最新データを取得します。プロバイダーがこの操作を行うための認証情報があることを確認してください。そのプロバイダーが **検出** で追加された場合には、 (**選択したインフラストラクチャープロバイダーの編集**) を使用して認証情報を追加します。

1. **コンピュート → インフラストラクチャー → プロバイダー** に移動します。
2. 更新するプロバイダーを選択します。
3. (構成) をクリックして、 (**リレーションシップと電源状態の更新**) を選択します。
4. **OK** をクリックします。

1.7. 複数のプロバイダーのタグ付け

プロバイダーを同時にまとめて分類するには、タグを適用します。

1. **インフラストラクチャー → プロバイダー** に移動します。
2. タグ付けするプロバイダーにチェックを付けます。
3. (**ポリシー**) をクリックして、 (**タグの編集**) を選択します。
4. **タグの割り当て** のセクションで、最初のリストからカスタマータグを選択し、2 番目のリストから割り当てる値を選択します。



5. 必要に応じて、追加のタグを選択します。(**Save**) をクリックします。

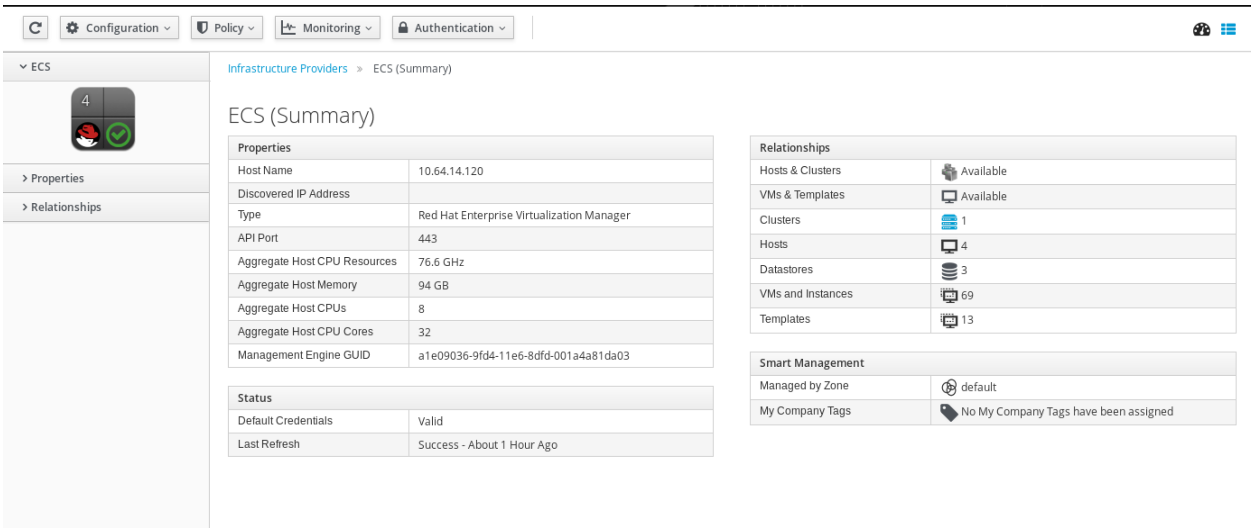
1.8. プロバイダーの表示

プロバイダーの一覧から、特定のプロバイダーをクリックして、レビューすることができます。これにより、プロバイダーの情報にアクセスするためのさまざまなオプションが表示されます。

インフラストラクチャープロバイダーの表示方法は、概要ビュー (デフォルト) とダッシュボードビューの 2 通りがあります。概要 とダッシュボード ボタンを使ってビューを切り替えます。

どちらの画面にもタスクバーがあり、**リロード**、**構成**、**ポリシー**、**監視**、および **認証** のボタンでプロバイダーを管理します。

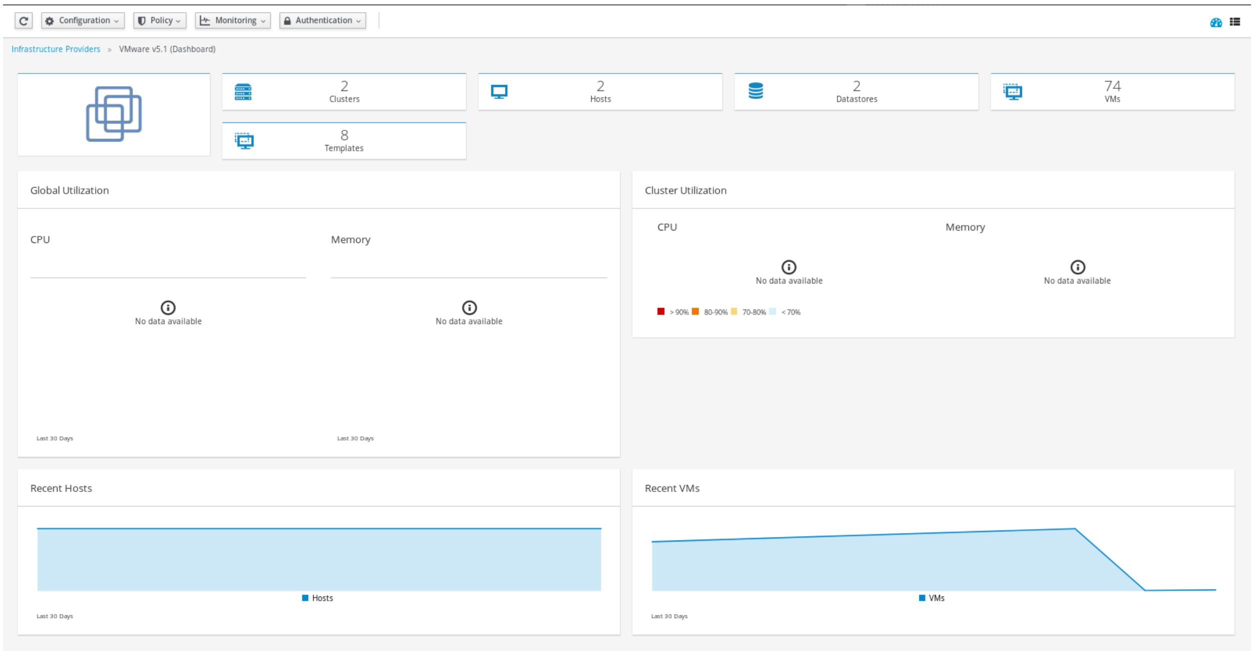
プロバイダー概要画面



プロバイダー概要画面では、テーブル形式で情報が表示されます。

- プロバイダーアコーディオン: プロバイダーの **プロパティー** と **リレーションシップ** についての詳細をサイドバーに表示します。
- プロバイダー概要: プロバイダーの **プロパティー**、**ステータス**、**リレーションシップ**、および **スマート管理** を表示します。**リレーションシップ** テーブル内のアイテムをクリックすると、そのエンティティーについての詳細情報が表示されます。

プロバイダーのダッシュボード画面



ダッシュボードでは、以下を確認できます。

- クラスター、ホスト、仮想マシン、テンプレート、データストア、リソースプール、その他のプロバイダー上のエンティティーの数。エンティティーをクリックすると、そのアイテムについての詳細情報が表示されます。
- CPU、メモリー、およびストレージの使用率
- ネットワーク I/O の統計値
- ホストおよび仮想マシンの傾向

ダッシュボードを表示するには、以下の手順に従います。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. 表示するインフラストラクチャープロバイダーをクリックします。
3. ダッシュボードビューにアクセスするには、 **(ダッシュボードビュー)** をクリックします。

概要ビューに戻るには、 **(概要ビュー)** をクリックします。

1.9. プロバイダーの削除

プロバイダーがデコミッションされた場合や、トラブルシューティングが必要な場合には、VMDB から削除する必要がある可能性があります。

プロバイダーを削除すると、Red Hat CloudForms コンソールからアカウント情報が削除され、その削除されたプロバイダー向けに生成されていたチャージバックレポートを含む関連履歴は表示できなくなります。また、Red Hat CloudForms がレコードのデータベースの場合には、プロバイダーを削除すると、そのプロバイダーに依存して正確で一貫した課金情報を取得している他のシステムで大きな問題となります。プロバイダーを削除する前には、すべての依存関係を慎重に確認してください。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。

2. 削除するプロバイダーのチェックボックスを選択します。

3. **(構成)** をクリックして、 **(VMDB からインフラストラクチャープロバイダーを削除)** を選択します。

4. **(OK)** をクリックします。

1.10. プロバイダーのタイムラインの表示

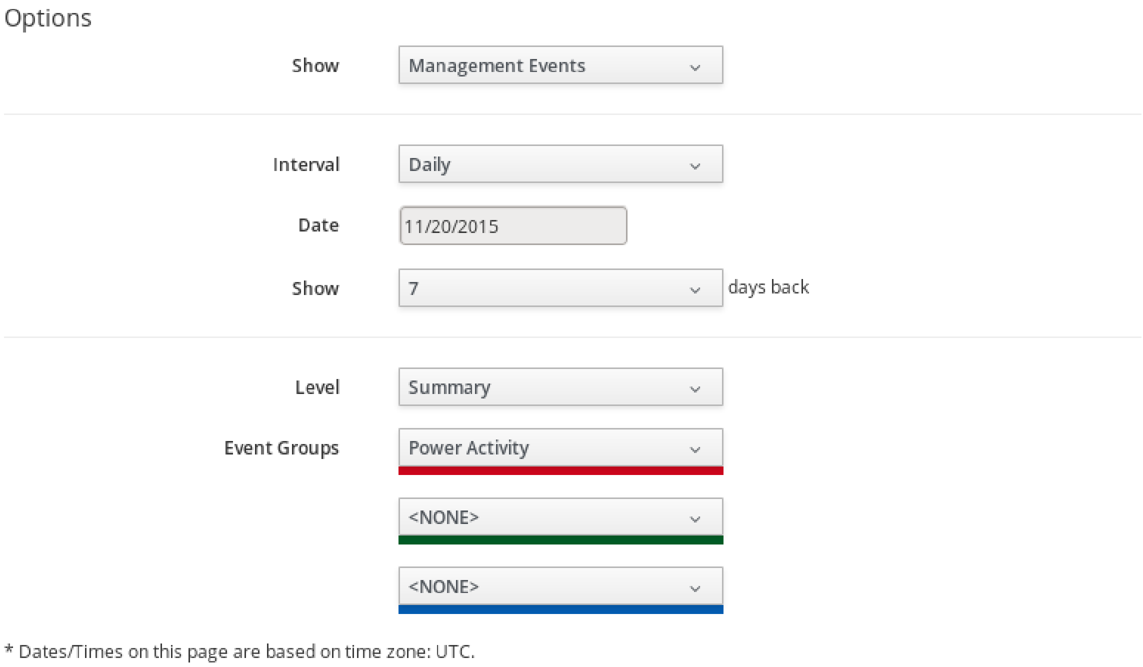
プロバイダーに登録されている仮想マシンのイベントのタイムラインを表示します。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。

2. プロバイダーをクリックします。

3. **(監視)** をクリックして、タスクバーから **(タイムライン)** をクリックするか、プロバイダーのアコーディオンメニューから **プロパティー** → **タイムライン** をクリックします。

4. **オプション** から、表示する期間や表示するイベントタイプをカスタマイズします。



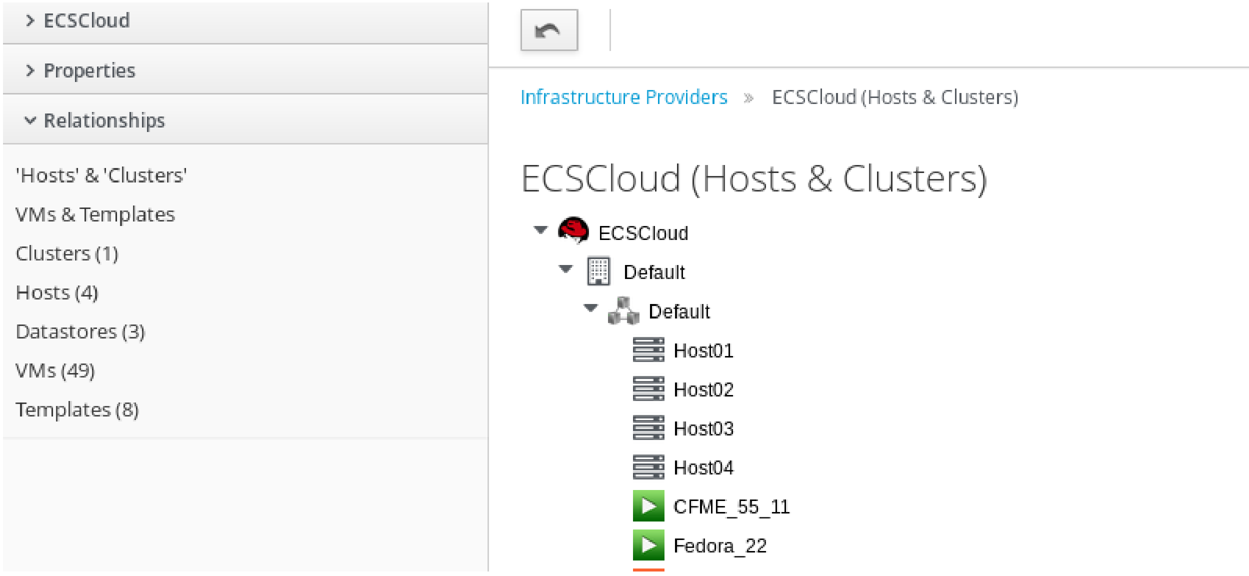
- **表示** を使用して、通常の管理イベントとポリシーイベントを選択します。
- **間隔** のドロップダウンを使用して、毎時または毎日のいずれかのデータポイントを選択します。
- **日付** で、表示するタイムラインの日付を入力します。
- 毎日のタイムラインを表示するように選択した場合は、**表示** を使用して、何日分遡るかを設定します。最大の履歴は 31 日です。
- 3 つの **イベントグループ** リストでは、異なるイベントグループを選択して表示することができます。それぞれ独自の色が使用されます。
- **レベル** の一覧から、**概要** イベントまたはイベントの **詳細** リストを選択します。たとえば、**電源オン** イベントの詳細レベルには、電源オンの要求、イベントの開始、実際の

電源オン イベントが含まれます。**概要** を選択した場合には、電源オンイベントのみがタイムラインに表示されます。

1.11. ホストとクラスターの表示

プロバイダーの概要 から、プロバイダーのホストとクラスターのツリービューにアクセスします。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. プロバイダーをクリックして、ホストとクラスターを表示します。
3. **リレーションシップ** のアコーディオンで、**ホスト & クラスター** をクリックします。



1.12. 仮想マシンとテンプレートの表示

プロバイダーの概要 から、プロバイダーの仮想マシンとテンプレートのツリービューにアクセスします。

1. **コンピュート** → **インフラストラクチャー** → **プロバイダー** に移動します。
2. プロバイダーをクリックして、仮想マシンとテンプレートを表示します。
3. アコーディオンメニューから、**リレーションシップ** をクリックして **仮想マシン & テンプレート** をクリックします。

第2章 設定管理プロバイダー

現在 Red Hat CloudForms には、複数の異なるプロバイダーが存在するために発生する混乱やエラーをなくために、設定項目とそれらに対する変更のレビューとモニタリングを行う 2 つの設定管理プロバイダーが統合されています。これらの設定システムは、設定項目のステータスと変更アクティビティーを記録および報告するのに使用されます。

2.1. RED HAT SATELLITE 6

Satellite 6 は、Puppet モジュールのセットを使用してホスト (仮想およびベアメタル) のプロビジョニングと設定を行う手段を提供するサブスクリプションおよびシステム管理のツールです。Red Hat CloudForms は Red Hat Satellite 6 サーバーと統合して、その特性を活用するための機能性を提供します。これには、以下が含まれます。

- 独立したホスト、ホストグループを使用してプロビジョニングされたホストを含む、Red Hat Satellite 6 サーバーインベントリーの監視
- 新規ホストグループへの既存のベアメタルシステムホストの再プロビジョニング
- ホストへの Red Hat CloudForms ポリシータグの適用

重要

Red Hat CloudForms は、Red Hat Satellite 6 環境内の既存のシステムを再プロビジョンするのみです。Red Hat Satellite 6 のベアメタル検出サービスは、今後のリリースで導入される予定です。

2.1.1. ワークフローの定義

本項では、以下のワークフローを使用します。

1. Red Hat Satellite 6 サーバーの情報を Red Hat CloudForms に追加します。
2. Red Hat CloudForms で、Red Hat Satellite 6 プロバイダーの状態を更新します。
3. Red Hat Satellite 6 から、再プロビジョニングする既存のベアメタルホストを選択します。
4. Red Hat Satellite 6 ホストにポリシータグを適用します。

2.1.2. ホストグループ階層の定義

Red Hat CloudForms は、ホストグループおよびホストリレーションシップ内の Red Hat Satellite 6 インフラストラクチャーを表示します。ホストグループは、ホストがそのグループに配置される際に継承するデフォルト値のセットを定義します。ホストは、1 つのホストグループにのみ属することができますが、ホストグループは、複数の階層に入れ子にすることができます。組織内の全ホストを表す**「ベース」**または**「親」**のホストグループを作成してから、ネストされたホストグループまたは**「子」**ホストグループを親の下に作成して、特定の設定を指定します。

2.1.3. Satellite 6 プロバイダーの追加

ベアメタルマシンのプロビジョニングを開始するには、Red Hat CloudForms に Red Hat Satelllite 6 プロバイダーを少なくとも 1 つ追加する必要があります。

1. **構成** → **管理** に移動します。
2. **構成** → **新規プロバイダーの追加** を選択します。
3. プロバイダーの **名前** を入力します。
4. プロバイダーの **URL** を入力します。これは、Satellite 6 サーバーのルート URL で、IP アドレスまたはホスト名を指定することができます (例: http://satellite6.example.com)。
5. プロバイダーとの間で暗号化された通信を使用する場合には、**ピア証明書の検証** を選択します。これには、Red Hat Satellite 6 プロバイダーからの **SSL 証明書** が必要です。
6. プロバイダー上のユーザーの **ユーザー名** を入力します。これには、管理権限を持つ Satellite 6 のユーザーが理想的です。
7. **パスワード** を入力して、**パスワードの確認** に再入力します。
8. **検証** をクリックして、Red Hat Satellite 6 サーバーとの接続をテストします。
9. **追加** をクリックして、設定を確認し、プロバイダーを保存します。

Red Hat CloudForms はデータベースに Satellite 6 プロバイダーを保存し、そのプロバイダー内で検出されたリソースの更新をトリガーします。

2.1.4. Satellite 6 プロバイダーの更新のトリガー

Satellite 6 プロバイダーは引き続き、Red Hat CloudForms とは無関係に新規ホストを作成することが可能です。Red Hat CloudForms アプライアンスは、自動更新期間が経過すると、これらの変更を検出しますが、自動更新を待たずに、更新を手動でトリガーすることも可能です。

1. **構成** → **管理** に移動します。
2. チェックボックスで Red Hat Satellite 6 プロバイダーを選択し、**構成** → **リレーションシップと電源状態の更新** をクリックします。これにより、更新がトリガーされます。
3. 更新が完了したら、対象の Red Hat Satellite 6 プロバイダーを選択して、そのプロバイダー内のホストグループの更新されたリストを確認します。

2.1.5. Red Hat Satellite 6 のコンテンツの表示

Red Hat CloudForms で Red Hat Satellite 6 プロバイダーのコンテンツを表示するには、2 つの方法があります。

- **プロバイダー**: このビューは、Red Hat Satellite 6 のコンテンツを、プロバイダーに属するホストグループと、各プロバイダーに属する個別のホストの階層として表示します。
- **構成済みシステム**: このビューは、Red Hat Satellite 6 サーバー上の全ホストの一覧を表示します。また、事前定義済みのフィルターを使用して、特定のマシンを整理する方法も提供します。

これらの 2 つのビューを切り替えるには、ユーザーインターフェースの左側にあるアコーディオンメニューを使用してください。

2.1.6. ベアメタルホストの再プロビジョニング

以下の手順では、既存のベアメタルシステムを新規ホストグループに再プロビジョニングする例を説明します。この例では、Red Hat Satellite 6 環境に以下の項目が必要です。

- Red Hat Satellite 6 サーバー内のホストオブジェクトとして保管された既存のベアメタルシステム。このシステムは、以下のいずれかを指定することができます。
  - ホストグループなしで以前にプロビジョニングされたスタンドアロンシステム
  - ホストグループを使用して以前にプロビジョニングされたシステム
- ターゲットホストグループ。このホストグループには、ホストを再プロビジョニングする際に適用するシステム設定が含まれます。これには、以下が含まれます。
  - 新規オペレーティングシステムをインストールした環境。新しいパーティションテーブルを含む。
  - Red Hat Satellite 6 サーバーが定義/管理する新規ネットワーク設定
  - Red Hat サブスクリプションへの登録と、ホストグループに割り当てられるリポジトリー
  - ホストグループに割り当てられる Puppet モジュールのアプリケーション

1. **構成** → **管理** に移動します。
2. 画面左側のアコーディオンメニューから **構成済みシステム** を選択し、システムの一覧を表示します。
3. 再プロビジョニングするホストを 1 つまたは複数選択します。
4. **ライフサイクル** → **構成済みシステムのプロビジョニング** を選択します。
5. **要求** タブで、以下の情報を入力します。
   a. **メールアドレス**
   b. **名**
   c. **姓**
   d. このフォームには、ユーザーが Red Hat CloudForms の管理者に特別な詳細情報を提供するためにプレーンテキスト形式の **メモ** を入力するオプションのフィールドと、管理者がユーザーのマネージャーの承認を得る必要がある場合のためにマネージャーの名前を入力するフィールドが含まれています。
6. **目的** のタブを選択し、そのシステムに適用する Red Hat CloudForms のポリシータグを選択します。
7. **カタログ** タブを選択します。この画面には、再プロビジョニングに選択したマシンと現在の情報を示す一覧が表示されます。**構成プロファイル** の一覧から **ターゲットホストグループ** を 1 つ選択します。Red Hat CloudForms は Red Hat Satellite と通信して、このホストグループから選択したホストに構成を適用し、システムを再プロビジョニングします。
8. **カスタマイズ** タブを選択します。この画面には、選択したシステムのカスタマイズ可能なフィールドがいくつか表示されます。**root パスワード** を変更したり、**ホスト名** や **IP アドレス** を変更することができます。Red Hat Satellite 6 にはこの情報が含まれているので、これらのフィールドはオプションであることに注意してください。このフィールドの設定により、ホストグループの設定が上書きされます。

重要

ベアメタルのプロビジョニングには Red Hat Satellite 6 が管理するネットワークへのアクセスが必要な点は変わりません。これは、Red Hat Satellite がベアメタルシステムの PXE ブート、キックスタート、および Puppet 設定を制御するためです。Red Hat CloudForms に入力する IP アドレスが、Red Hat Satellite 6 のメインサーバーまた Red Hat Satellite 6 Capsule サーバー提供される DHCP サービスにアクセスできることを確認してください。

9. **カスタマイズ** タブを選択します。この画面では、承認直後にプロビジョニングプロセスを直ちに開始するか、スケジュールを使用して実行することができます。**スケジュール** をクリックして、プロビジョニングのスケジュールに使用する日時を表示します。
10. **送信** をクリックします。

Red Hat CloudForms アプライアンス上の要求の設定によっては、このプロビジョニング要求に管理者の承認が必要な場合があります。承認が必要でない場合には、プロビジョニング要求はスケジュールの選択に応じて開始されます。

注記

以前にプロビジョニングされたホストは、ブートメニューから手動で PXE ブートを選択しなければ、ハードディスクでブートして、再プロビジョニングされない可能性があります。

2.1.7. ベアメタルホストのタグ付け

Red Hat CloudForms はタグ付けによって Red Hat Satellite 6 からのベアメタルシステムのポリシー設定を制御することも可能です。タグ付けにより、システムのセットに必要なポリシールールを定義するのに役立つメタデータのレベルがアタッチされます。

1. **構成** → **管理** に移動します。
2. 画面左側のアコーディオンメニューから **構成済みシステム** を選択し、システムの一覧を表示します。
3. タグ付けするホストを 1 つまたは複数選択します。
4. **ポリシー** → **タグの編集** を選択します。
5. **タグの割り当て** で **割り当てるカスタマータグの選択** からタグを選択して、**割り当てる値の選択** から値を選択します。たとえば、`Location` をタグに、`Chicago` を値に選択すると、このシステムをシカゴにあるものとしてタグを付けることができます。選択が完了すると、ユーザーインターフェースは自動的にこのタグと値を以下のテーブルに追加します。
6. **保存** をクリックします。

ベアメタルシステムがポリシータグのセットで設定されました。

2.2. ANSIBLE TOWER

Ansible Tower は、Red Hat CloudForms に統合された管理ツールで、インフラストラクチャーの運

用の自動化を支援するために設計されています。Red Hat CloudForms では、サービスカタログと自動化を使用して Ansible Tower のジョブを実行することができます。設定は、プレイブックを使用して Ansible Tower 内で行われるので、Red Hat CloudForms ではカスタムの設定や Ruby のスクリプトは必要ありません。

既存の Ansible プレイブックの大型のライブラリーを Red Hat CloudForms のステートマシンとして使用すると、Red Hat CloudForms 環境におけるバックアップやパッケージの更新、メンテナンスなどのタスクを自動化することができます。これには、Red Hat Satellite エージェントを必要に応じてベアメタルマシン上にデプロイする操作も含まれます。これは、特に多数の仮想マシンやインスタンスのある大型環境全体に変更を迅速に適用するのに特に役立ちます。Ansible Tower を使用すると、Ansible のプレイブックの実行をスケジュールして、現在および過去の結果をモニタリングし、トラブルシューティングを行ったり、問題が発生する雨に特定することができます。

Red Hat CloudForms を Ansible Tower プロバイダーとともに使用する場合の基本ワークフローは以下のとおりです。

1. 特定のタスクを実行する Ansible プレイブックを作成します。
2. 新しい Ansible Tower Job テンプレートは、プレイブックから作成され、Red Hat CloudForms によって取得されます。
3. Ansible Tower Job テンプレートから、Red Hat CloudForms の新規カタログ項目を作成します。また、オプションとして、ユーザーが必要に応じてパラメーターを入力することができるサービスダイアログを作成します。
4. ユーザーは Red Hat CloudForms のユーザーインターフェースからサービスをオーダーして、追加の引数 (例: 特定の仮想マシンセットで実行するタスクを制限するなど) を記入します。
5. ジョブが実行されます。

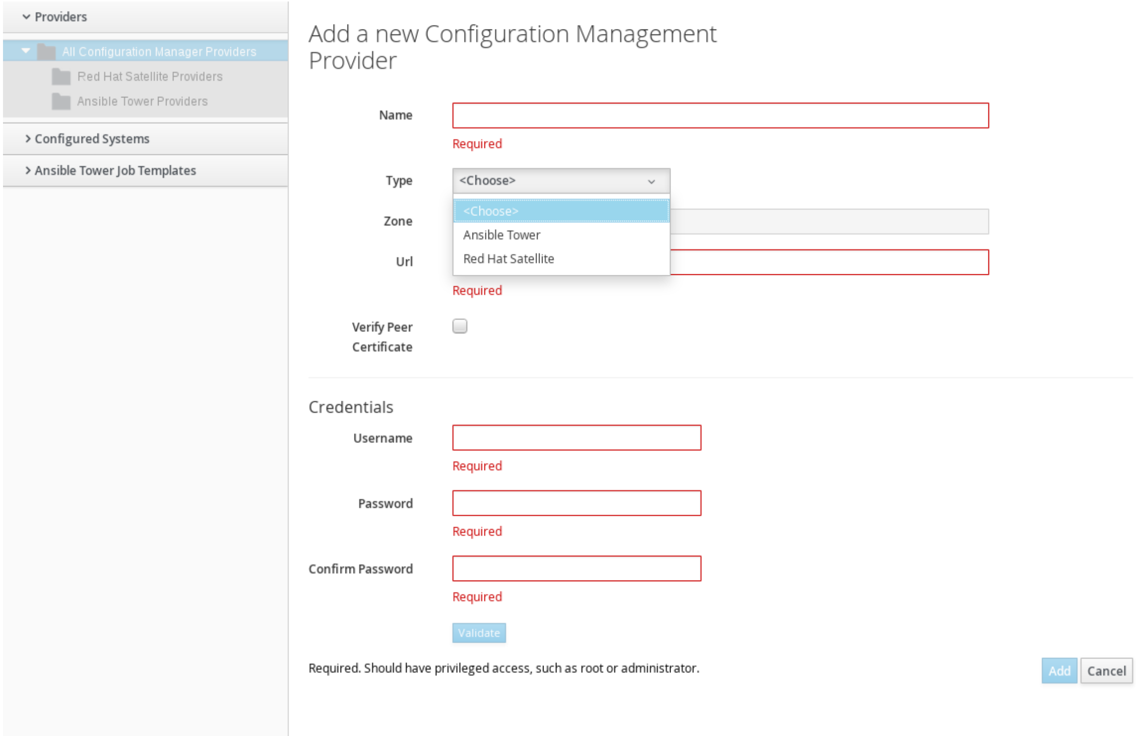
注記

Ansible プレイブックについての詳しい情報は、Ansible プレイブックのドキュメント を参照してください。

2.2.1. Ansible Tower プロバイダーの追加

Red Hat CloudForms から Ansible Tower インベントリーにアクセスするには、Ansible Tower をプロバイダーとして追加する必要があります。

1. **構成** → **管理** → **プロバイダー** に移動します。
2. **構成** で **新規プロバイダーの追加** をクリックします。
3. **新規構成管理プロバイダーの追加** のセクションで以下のように設定します。



a. 新規プロバイダーの **名前** を入力します。

b. **タイプ** のフィールドで、一覧から **Ansible Tower** を選択します。

c. Ansible Tower サーバーの **URL** ロケーションまたは IP アドレスを入力します。

4. 必要な場合には、**ピア証明書の検証** のチェックボックスを選択します。

5. **認証情報** のセクションで **ユーザー名**、**パスワード**、 **パスワードの確認** のフィールドに入力します。

6. **追加** をクリックします。

Ansible Tower プロバイダーを追加した後には、リレーションシップと電源状態を更新して、現在のインベントリーが表示されるようにします。

2.2.2. Ansible Tower プロバイダーの更新

インベントリー、ホスト、仮想マシン、クラスターを含む既存の Ansible Tower の構成管理プロバイダーに関連した全項目のリレーションシップを更新します。

Red Hat CloudForms からインベントリーを更新するか、Ansible Tower 内のインベントリーグループの **Update on Launch** オプションを有効にします。**Update on Launch** オプションにより、プレイブックから Ansible Tower ジョブを起動する前に、動的インベントリースクリプトを使用して Ansible Tower は自動的にインベントリーを更新することができます。詳しくは、Ansible Tower のドキュメント を参照してください。

重要

多数の仮想マシンまたはインスタンスがあるプロバイダーから情報を取得するには長時間かかる場合があります。Ansible Tower の動的インベントリースクリプトを編集して、更新を特定の項目に限定して、更新時間を短縮することが可能です。

Red Hat CloudForms で Ansible Tower プロバイダーのインベントリーを更新するには、以下のステップを実行します。

1. **構成** → **管理** → **プロバイダー** に移動します。
2. **すべての Ansible Tower プロバイダー** で更新する Ansible Tower プロバイダーのチェックボックスを選択します。
3. (**構成**) をクリックして、 (**リレーションシップと電源状態の更新**) を選択します。
4. **OK** をクリックします。

Red Hat CloudForms は次に Ansible Tower API に対してクエリーを実行し、利用可能なホストと Job テンプレートのインベントリーを取得します。

2.2.3. Ansible Tower プロバイダーとインベントリーの表示

Red Hat CloudForms は、Ansible Tower からインベントリーを自動的に更新します。これには、システムグループ (Ansible Tower 内のインベントリー)、個々のシステムに関する基本情報、サービスカタログまたは自動化から実行される、利用可能な Ansible Tower Job テンプレートが含まれます。

注記

Red Hat CloudForms で Ansible Tower のインベントリーと Job テンプレートを表示およびアクセスするには、まず最初にそれらを Ansible Tower で作成する必要があります。

Ansible Tower プロバイダーとインベントリーの一覧を表示するには、以下のステップを実行します。

1. **構成** → **管理** → **プロバイダー** に移動します。
2. **すべての構成マネージャープロバイダー** で **Ansible Tower プロバイダー** のアコーディオンメニューを選択してプロバイダーの一覧を表示します。
3. お使いの Ansible Tower プロバイダーを選択して、その Ansible Tower システム上にあるインベントリーグループを展開し、一覧表示します。インベントリーグループを展開すると、各グループに含まれるシステムと、それらのシステムの構成についての詳細情報が表示されます。

同様に、検出された Job テンプレートは **構成** → **管理** → **Ansible Tower Job テンプレート** のアコーディオンメニューを展開すると、そのプロバイダーの下に表示されます。

2.2.4. Ansible Tower 構成済みシステム

Ansible Tower のインベントリーを表示するには、以下のステップを実行します。

1. **構成** → **管理** → **構成済みシステム** に移動します。
2. **すべての構成済みシステム** で **Ansible Tower 構成済みシステム** を選択して一覧を表示します。

2.2.5. サービスカタログからの Ansible Tower Job テンプレートの実行

2.2.5. サービスカタログからの Ansible Tower Job テンプレートの実行

Ansible Tower Job テンプレートからサービスカタログ項目を作成して、Red Hat CloudForms から Ansible Tower プレイブックを実行することができます。

重要

まず最初に、Ansible Tower で Job テンプレートを作成する必要があります。作成したテンプレートは、Ansible Tower プロバイダーのインベントリーを更新すると、Red Hat CloudForms によって自動的に検出されます。

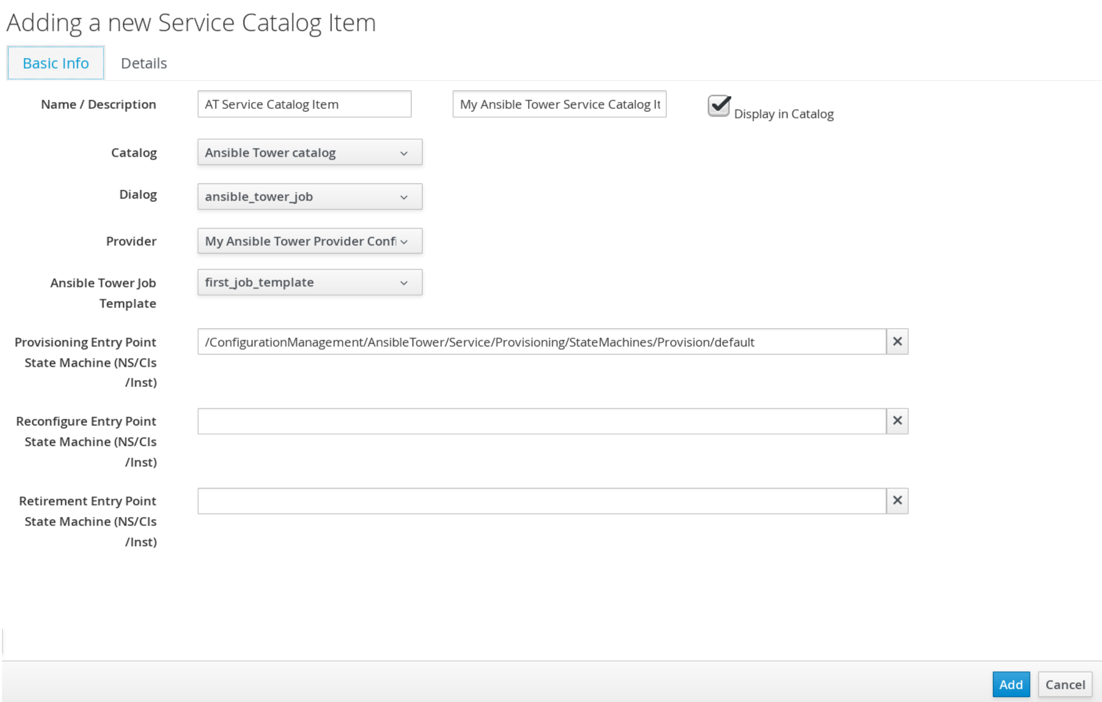
最初にカタログを作成します。

1. **サービス** → **カタログ** に移動します。
2. (**構成**) をクリックして、 (**新規カタログの追加**) を選択します。
3. カタログの **名前** と **説明** を入力します。
4. **追加** をクリックします。

次に Ansible Tower サービスカタログ項目を作成します。

1. **構成** → **管理** に移動します。
2. **Ansible Tower Job テンプレート** をクリックして Ansible Tower Job テンプレートを選択します。
3. (**構成**) をクリックして、 (**この Job テンプレートからサービスダイアログを作成する**) を選択します。
4. **サービスダイアログ名** (例: **ansible_tower_job** など) を入力して **保存** をクリックします。
5. **サービス** → **カタログ** に移動して、**カタログ項目** をクリックします。
6. (**構成**) をクリックして (**新規カタログ項目の追加**) を選択し、少なくとも以下の情報を指定して新規カタログ項目を作成します。
   - **カタログ項目タイプ** には **Ansible Tower** を選択します。
   - サービスカタログ項目の **名前** を入力します。
   - **カタログ内に表示** を選択します。
   - **カタログ** で、以前に作成したカタログを選択します。
   - **ダイアログ** で以前に作成したサービスダイアログ (この例では **ansible_tower_job**) を選択します。プレイブックにユーザーからの追加のパラメーターが必要ない場合には、**ダイアログなし** を選択することが可能です。タスク実行時にユーザーに追加の情報の入力を要求するには、**サービスダイアログ** を選択する必要があります。
   - **プロバイダー** でお使いの Ansible Tower プロバイダーを選択すると、**Ansible Tower Job テンプレート** オプションが表示され、**プロビジョニングのエントリーポイントのステートマシン** が自動的に設定されます。

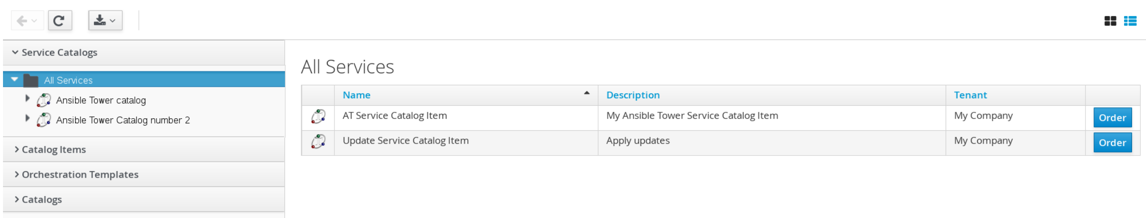
- 一覧から必要な **Ansible Tower Job テンプレート** を選択します。通常、これには、サービスダイアログの作成に使用した Ansible Tower Job テンプレートを選択します。



7. **追加** をクリックします。作成したカタログ項目が **全サービスカタログ項目** の一覧に表示されます。

Ansible Tower Job を実行するには、以下のステップを実行します。

1. **サービスカタログ** → **Ansible Tower カタログ** に移動します。



2. カタログアイテムの **オーダー** をクリックします。

3. 要求するパラメーターを入力して **送信** をクリックします。

Red Hat CloudForms の **要求** キューのページが開き、ジョブのステータスが表示されます。

サービス項目の詳細は、Red Hat CloudForms の **サービス** → **マイサービス** で確認することができます。

注記

1 回ごとに単一のジョブを実行する代わりに、複数のサービスカタログ項目をカタログバンドルとしてグループ化して、複数のジョブテンプレートを使用する単一のデプロイメントを作成することができます。詳しい情報は、**『仮想マシンとホストのプロビジョニング』** の「カタログとサービス」を参照してください。

2.2.6. カスタムの自動化ボタンを使用した Ansible Tower Job の実行

Red Hat CloudForms では、自動化のカスタムボタンを使用して、Ansible Tower のジョブを仮想マシンまたはインスタンスで実行することができます。

Ansible Tower のジョブは、ユーザーによる追加の設定を必要としないようにカスタマイズ不可とするか、ユーザーがパラメーター (例: インストールするパッケージ名など) を指定できるようにすることができます。ダイアログが含まれている Ansible Tower のジョブでは、Red Hat CloudForms はユーザーからの追加情報を受け入れ、自動化で適切な API コールに追加してから、Ansible Tower に送信します。

前提条件

Ansible Tower Job を実行する自動化ボタンを作成する前に、以下の項目を設定する必要があります。

- Ansible Tower 内の Ansible プレイブック。手順については、Ansible Tower documentation を参照してください。
- Ansible Tower は、Red Hat CloudForms でデプロイされた仮想マシンまたはインスタンスに IP レベルで接続できる必要があります。
- 仮想マシンテンプレートには、Ansible Tower 環境のパブリック SSH キーを注入する必要があります。クラウドインスタンスの場合には、`cloud-init` を使用可能で、イメージを再ビルドせずにパブリック SSH キーを渡すことができます。
- 使用する動的インベントリースクリプトは、UUID を追記せずに、Red Hat CloudForms で保管されている通りの仮想マシン名を返すように設定する必要があります。

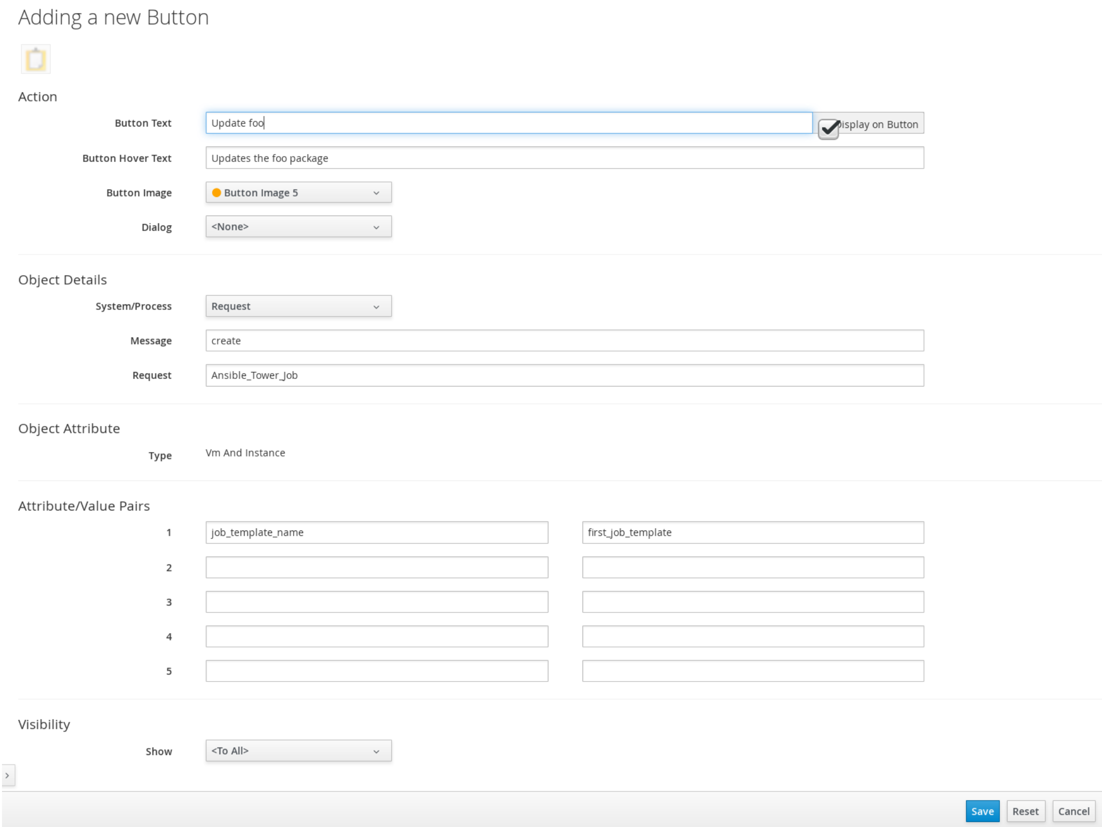
カスタムの自動化ボタンを使用した **Ansible Tower** ジョブの実行

仮想マシンまたはインスタンス上で Ansible Tower ジョブを実行するためのカスタムボタンを設定するには、まず最初にボタンを作成します。

1. **自動化** → **カスタマイズ** に移動します。
2. **ボタン** のアコーディオンメニューをクリックします。
3. **仮想マシンおよびインスタンス** → **未割り当てボタン** をクリックして、仮想マシンまたはインスタンス上で実行するボタンを設定します。
4. (**構成**) をクリックして (**新規ボタンの追加**) を選択します。
   - **新規ボタンの追加** の画面で、必要に応じて **アクション** パラメーターを設定します。プレイブックで追加のパラメーターが必要ない場合には、**ダイアログ** を空白のままにすることができます。タスクの実行時にユーザーが追加の情報を入力するように要求するには、**サービスダイアログ** を選択する必要があります。
   - **オブジェクト詳細** フィールドに以下にあげる要求の詳細を設定します。
     - **システム/プロセス** には、**要求** を選択します。
     - **メッセージ** には **作成** を入力します。
     - **要求** には、**Ansible_Tower_Job** と入力します。
   - **属性と値のペア** は、次のパラメーターで設定します。
     - **job_template_name** には、ボタンに関連付ける Ansible Tower Job テンプレート名を指定します。**job_template_name** フィールドは必須です。その他のパラメー

を指定します。**job_template_name** フィールドは必須です。その他のパラメーターは Tower のジョブダイアログで指定します。

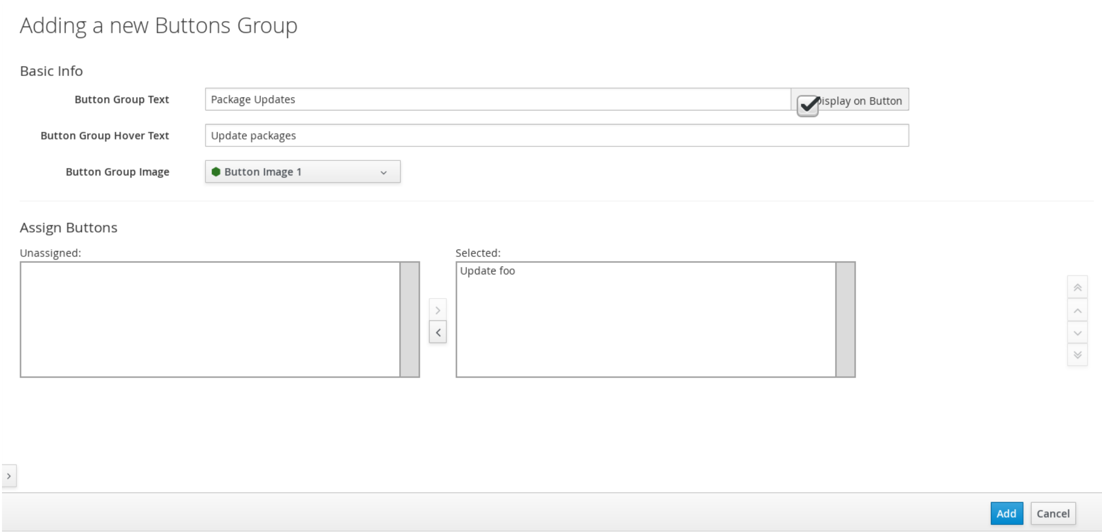
- 全ユーザーに対して **可視性** を設定するか、必要に応じてロール別に可視性を制限します。



- **追加** をクリックします。

新規ボタンを割り当てる既存のボタングループがない場合には、新しいボタングループを作成します。

1. **自動化** → **カスタマイズ** から **ボタン** → **仮想マシンおよびインスタンス** → **新規ボタングループの追加** に移動し、以下の設定を行います。
   - 必要に応じて **基本情報** を設定します。たとえば、ボタングループの名前を **`VM Actions`** に指定します。
   - **ボタンの割り当て** で、前のステップで作成したボタンを **未割り当て** の一覧から選択し、 をクリックして **選択内容** に移動します。



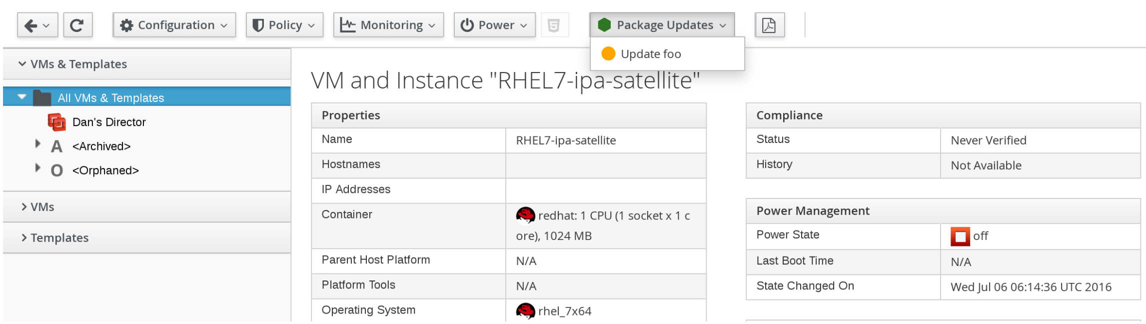
- **追加** をクリックします。

ボタンを既存のボタングループに割り当てるには、以下のステップを実行します。

1. **ボタン** → **仮想マシンおよびインスタンス** → **VM Actions** → **このボタングループの編集** に移動します。
2. **ボタンの割り当て** で、前のステップで作成したボタンを **未割り当て** の一覧から選択し、 をクリックして **選択内容** に移動します。
3. **追加** をクリックします。

ボタンを使用して Ansible Tower のジョブを仮想マシンで実行するには、以下のステップに実行します。

1. **コンピュート** → **インフラストラクチャー** → **仮想マシン** に移動します。
2. Ansible Tower ジョブテンプレートを実行する仮想マシンを選択します。
3. **VM Actions** ボタンをクリックして、作成したボタンを表示します。一覧から、Ansible Tower Job テンプレートを実行するためのボタンをクリックします。



4. **送信** をクリックしてジョブを実行します。

Red Hat CloudForms はジョブが実行されたことを確認するメッセージを表示します。

ボタンの作成時にサービスダイアログを選択した場合には、Red Hat CloudForms はタスクを完了するためのパラメーターを入力するように要求します。必要なパラメーターを入力した後には、Red Hat CloudForms で **要求** のページが表示されます。

サービス項目の詳細は、Red Hat CloudForms の **サービス** → **マイサービス** で確認することができます。

第3章 クラウドプロバイダー

Red Hat CloudForms においてクラウドプロバイダーとは、Red Hat CloudForms アプライアンスを追加して環境内のリソースの管理やそれらのリソースとの対話を行うことができるクラウドコンピューティング環境のことを指します。本章では、Red Hat CloudForms に追加可能なクラウドプロバイダーの異なるタイプとそれらの管理方法について説明します。

3.1. OPENSTACK プロバイダー

3.1.1. OpenStack プロバイダーの追加

Red Hat CloudForms はOpenStack **`admin`** テナントの運用をサポートしています。OpenStack プロバイダーの **`admin`** ユーザーは OpenStack **`admin`** テナントのデフォルト管理者なので、Red Hat CloudForms で OpenStack プロバイダーを作成する際にはこのユーザーを選択してくださ。**`admin`** の認証情報を使用する場合には、Red Hat CloudForms 内のユーザーは **`admin`** テナント内にプロビジョニングを行い、**`admin`** テナントに関連付けられたイメージ、ネットワーク、インスタンスを確認することができます。

注記

OpenStack クラウドもしくはインフラストラクチャープロバイダーを追加する際には、**テナントマッピング** を Red Hat CloudForms で有効にして、そのプロバイダーから既存のテナントにマッピングするようにできます。つまり、Red Hat CloudForms が既存の各 OpenStack テナントに一致する新たなクラウドテナントを作成することになります。この新規作成のクラウドテナントと対応する OpenStack テナントは、同一のユーザーメンバーシップ、クォータ、アクセス/セキュリティールール、リソース割り当てを持つことになります。

プロバイダーのリフレッシュ中に、Red Hat CloudForms は OpenStack のテナントリストの変更もチェックします。Red Hat CloudForms は新しいテナントに一致する新規クラウドテナントを作成し、存在しなくなった OpenStack テナントに対応するクラウドテナントを削除します。Red Hat CloudForms は、OpenStack テナントになされた変更を対応するクラウドテナントにも複製します。

注記

Red Hat CloudForms でイベントのモニタリングに Telemetry サービスを使用するか、Advanced Message Queueing Protocol (AMQP) を使用するかを設定することができます。Telemetry を選択する場合には、最初に **ceilometer** サービスをオーバークラウド上でイベントを保管するように設定する必要があります。手順については、「オーバークラウドでイベントを保管するための設定」を参照してください。

詳しい情報は、Red Hat OpenStack Platform **『アーキテクチャーガイド』**の「OpenStack Telemetry (ceilometer)」 のセクションを参照してください。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規クラウドプロバイダーの追加**) を選択します。
3. プロバイダーの **名前** を入力します。

4. **タイプ** のドロップダウンメニューから **OpenStack** を選択します。

5. 一覧から適切な **API バージョン** を選択します。デフォルトは **`Keystone v2`** です。

   `Keystone v3` を選択した場合には、Red Hat CloudForms が使用する必要のある **`Keystone V3 Domain ID`** を入力します。これは、後ほど **Default** タブで指定するユーザーアカウントのドメインです。プロバイダーでドメインが設定されていない場合には、**default** と入力します。

   > **注記**
   >
   > Keystone API v3 を使用する場合には、ドメインは OpenStack 内のサービスエンティティーの管理の境界を決定するのに使用されます。ドメインにより、ドメイン固有の構成やセキュリティーオプションを設定するなどのさまざまな目的でユーザーをグループ化することができます。詳しい情報は、Red Hat OpenStack Platform **『アーキテクチャーガイド』** の「OpenStack Identity (keystone)」のセクションを参照してください。

6. デフォルトでは、**テナントマッピング** は無効になっています。有効にするには、**テナントマッピングの有効化** を **Yes** 設定します。

7. プロバイダー用に適切な **ゾーン** を選択します。デフォルトでは、ゾーンは **default** に設定されます。

   > **注記**
   >
   > 詳しい情報は、Red Hat OpenStack Platform **『アーキテクチャーガイド』** の「OpenStack Compute (nova)」のセクションでホストアグリゲートとアベイラビリティーゾーンの定義を参照してください。

8. **デフォルト** タブの **エンドポイント** のセクションで、OpenStack プロバイダーのホストと認証の詳細を設定します。

   a. **または IPv4 または IPv6 アドレス** に OpenStack Keystone サービスのパブリック IP または完全修飾ドメイン名を入力します。

      > **注記**
      >
      > ここで必要なホスト名は、director によって生成される **~/overcloudrc**ファイル (Red Hat OpenStack Platform **『director のインストールと使用方法』** の「オーバークラウドへのアクセス」のセクションを参照)または Packstack によって生成される **~/keystonerc_admin** ファイル (「OpenStack の評価: 単一ノードデプロイメント」を参照) の **OS_AUTH_URL** の値でもあります。

   b. **API ポート** で、OpenStack Keystone サービスに使用するパブリックポートを設定します。デフォルトでは OpenStack はこのサービスにポート 5000 を使用します。

   c. OpenStack プロバイダーとの認証に使用する適切な **セキュリティープロトコル** を選択します。

d. **ユーザー名** のフィールドで、OpenStack 環境のユーザー名を入力します。

> **重要**
>
> Keystone v3 認証を使用する環境では、関連するドメインの **admin** ロールがユーザーに付与されている必要があります。

e. **パスワード** および **パスワードの確認** フィールドで、ユーザーのパスワードを入力します。

f. **検証** をクリックして、Red Hat CloudForms が OpenStack プロバイダーに接続できることを確認します。

9. 次に、Red Hat CloudForms が OpenStack プロバイダーからイベントを受信する方法を設定します。**エンドポイント** セクションの **イベント** タブをクリックして設定を開始します。

   - OpenStack プロバイダーの Telemetry サービスを使用するには、**Ceilometer** を選択します。使用する前には、プロバイダーをあらかじめ適切に設定しておく必要があります。詳しくは、「オーバークラウドでイベントを保管するための設定」を参照してください。

   - 代わりに AMQP Messaging バスを使用する場合には、**AMQP** を選択します。その場合には、**ホスト名 (または IPv4 または IPv6 アドレス)** (**エンドポイント** の **イベント** タブ) に AMQP ホストのパブリック IP または修飾ドメイン名を入力します。

     - **API ポート** には、AMQP で使用するパブリックポートを設定します。デフォルトでは、OpenStack はこのホストにポート 5672 を使用します。

     - **ユーザー名** のフィールドには、アクセス権限のある OpenStack ユーザー名を入力します (例: **admin**)。次に、 対応するパスワードを **パスワード** と **パスワードの確認** のフィールドに入力します。

     - **検証** をクリックして認証情報を確認します。

10. クラウドプロバイダーを設定した後には、**追加** をクリックします。

> **注記**
>
> OpenStack 環境からインベントリーとメトリックを収集するために、Red Hat CloudForms アプライアンスは、OpenStack 環境の adminURL エンドポイントが非プライベートのネットワークにあることを要件とします。このため、OpenStack adminURL エンドポイントには `192.168.x.x` 以外の IP アドレスを割り当てる必要があります。また、すべての Keystone エンドポイントがアクセス可能である必要があります。アクセスできない場合には、更新が失敗します。

3.1.1.1. オーバークラウドでイベントを保管するための設定

デフォルトでは、Telemetry サービスは、Red Hat OpenStack Platform 環境の他のサービスによって生成されたイベントは保管しません。以下の手順では、OpenStack クラウドプロバイダー上の Telemetry サービスがそれらのイベントを保管するようにする方法を説明します。これにより、イベントは、Red Hat OpenStack Platform 環境がクラウドプロバイダーに追加されると Red Hat CloudForms に表示されるようになります。

1. アンダークラウドホストにログインします。

2. **ceilometer.yaml** という名前の環境ファイルを作成し、以下の内容を追加します。

```
parameter_defaults:
  CeilometerStoreEvents: true
```

3. この環境ファイルを **overcloud deploy** コマンドで指定します。

```
# openstack overcloud deploy --templates -e ~/ceilometer.yaml
```

OpenStack クラウドプロバイダーがアンダークラウドでデプロイされたのではない場合には、手動で設定することができます。そのためには、以下のステップを実行します。

1. コントローラーノードにログインします。

2. **/etc/ceilometer/ceilometer.conf** を編集して以下のオプションを指定します。

```
store_events = True
```

3. **/etc/heat/heat.conf** を編集して以下のオプションを指定します。

```
notification_driver=glance.openstack.common.notifier.rpc_notifier
notification_topics=notifications
```

4. **/etc/nova/nova.conf** を編集して以下のオプションを指定します。

```
notification_driver=messaging
notification_topics=notifications
```

5. Compute サービスおよび Orchestration サービスを再起動します。

```
# systemctl restart openstack-heat-api.service \
  openstack-heat-api-cfn.service \
  openstack-heat-engine.service \
  openstack-heat-api-cloudwatch.service
```

```
# systemctl restart openstack-nova-compute.service
```

3.2. AZURE プロバイダー

3.2.1. Azure プロバイダーの追加

Red Hat CloudForms は Microsoft Azure プロバイダーをサポートするようになりました。

重要

Red Hat CloudForms で Microsoft Azure を認証できるようにするには、前提条件となる一連のステップを Azure ポータルで実行する必要があります。「Create Active Directory application and service principal account using the Azure portal」を参照してください。このリンク先では、Azure Active Directory (AAD) の設定方法や、組織で開発するアプリケーションの作成、また Red Hat CloudForms のプロバイダーとして Azure インスタンスに接続できるようにするアプリケーションを追加するためのテナント ID、クライアント ID、クライアントキーの取得方法を説明しています。上記のリンクでは、**アプリケーションをロールに割り当てる** 際にステップ 3 では **Contributor** ロールを選択し、**Reader** ロールは選択しないように注意することが重要となります。また、これらのステップはすべて、Azure Resource Manager または Service Manager (Classic) モードを使用して実行可能な点にも注意してください。

Azure ポータルを使用してサービスプリンシパルアカウント (ディレクトリー内のアプリケーションのインスタンス) が作成されたら、Azure Active Directory (AAD) モジュール内で以下の 3 つの情報が利用可能になります。

- テナント ID
- クライアント ID
- クライアントキー

これで、以下の手順に従って上記の項目を Red Hat CloudForms に実装し、Azure クラウドプロバイダーを追加することができるようになりました。

Azure クラウドプロバイダーを追加する手順:

注記

Azure クラウドプロバイダーを追加する際には、指定可能なリージョンの一覧からリージョンを 1 つ選択します。選択したリージョーンに対してプロバイダーが 1 つ作成されます。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規クラウドプロバイダーの追加**) を選択します。
3. プロバイダーの **名前** を入力します。
4. **タイプ** の一覧から **Azure** を選択します。
5. **リージョン** の一覧からリージョンを 1 つ選択します。
6. **テナント ID** を入力します。
7. **ゾーン** を入力します。
8. **認証情報** のセクションで、**クライアント ID** と **クライアントキー** を入力してから **検証** をクリックします。
9. **追加** をクリックします。

3.2.2. Azure プロバイダーの検出

3.2.2. Azure プロバイダーの検出

Red Hat CloudForms は、全リージョンにわたる Microsoft Azure プロバイダーのセットを検出する機能を提供します。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**クラウドプロバイダーの検出**) を選択します。
3. **タイプの検出** の一覧から **Azure** を選択します。
4. 認証情報のセクションで、Azure の **クライアント ID**、**クライアントキー**、**Azure テナント ID**、および テナントの **サブスクリプション ID** を入力します。
5. **開始** をクリックします。

3.3. AMAZON EC2 プロバイダー

3.3.1. Amazon EC2 プロバイダーの権限

Red Hat は、CloudForms に Amazon EC2 をクラウドプロバイダーとして追加する場合には、Amazon EC2 の **パワーユーザー** 用の Identity and Access Management (IAM) ポリシーを使用することを推奨します。このポリシーは、**パワーユーザー** グループ内のメンバーに、ユーザー管理以外の AWS サービスへの完全なアクセスを許可します。このため、CloudForms API ユーザーは全 API 機能にアクセスできますが、ユーザーの権限を変更することはできません。

自動化のスクリプトは直接 AWS SDK にアクセスして新しいアプリケーション機能を作成するので、API アクセスをさらに制限してしまうと、自動化機能が限定されてしまいます。

CloudForms API がアクセスする主要な AWS サービスには、以下が含まれます。

- Elastic Compute Cloud (EC2)
- CloudFormation
- CloudWatch
- Elastic Load Balancing
- Simple Notification Service (SNS)
- Simple Queue Service (SQS)

3.3.2. Amazon EC2 プロバイダーを追加します。

初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、 以下の手順で Amazon EC2 クラウドプロバイダーを追加します。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規クラウドプロバイダーの追加**) を選択します。
3. プロバイダーの **名前** を入力します。
4. **タイプ** の一覧から **Amazon EC2** を選択します。

5. **Amazon Region** を選択します。

6. 複数の **ゾーン** が利用可能な場合には、適切なゾーンを選択します。

7. Amazon AWS アカウントの **セキュリティー認証情報** で **アクセスキー** を生成します。**アクセスキー ID** は **ユーザー ID** として機能し、**シークレットアクセスキー** は **パスワード** として機能します。

8. **検証** をクリックして認証情報を検証します。

9. **追加** をクリックします。

3.3.3. Amazon EC2 クラウドプロバイダーの検出

Red Hat CloudForms は、特定の Amazon EC2 アカウント情報のセットに関連付けられたクラウドプロバイダーを検出する機能を提供します。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。

2. (**構成**) をクリックして (**クラウドプロバイダーの検出**) を選択します。

3. **タイプの検出** の一覧から Amazon EC2 を選択します。

4. Amazon EC2 **ユーザー ID** と **パスワード** を入力します。**パスワードの確認** フィールドにパスワードを再入力します。

5. **開始** をクリックします。

3.3.4. Amazon EC2 からのパブリック AMI の有効化

デフォルトでは、Amazon EC2 プロバイダーからのパブリック AMI は Red Hat CloudForms には表示されません。これらのイメージが表示されるようにするには、アプライアンスのメインの設定ファイルを編集する必要があります。

1. 設定メニューから **構成** → **ゾーン** → **詳細** をクリックします。

2. **ファイル** 一覧から編集する設定ファイルを選択します。自動的に選択されていない場合には **EVM Server Main Configuration** を選択します。

3. **get_public_images** のパラメーターを設定します。

    a. パブリックイメージが表示されるようにするには、**get_public_images: true** にパラメーターを設定します。

    b. パブリックイメージが表示されないようにするには、**get_public_images: false** にパラメーターを設定します。

3.3.5. AWS Config の通知の有効化

Amazon の AWS Config は、Simple Notification Service (SNS) を使用して、リージョン内の変更をサブスクライバーに通知します。Red Hat CloudForms は AWS Config の差分の SNS サービスをサブスクライブして、その差分を Red Hat CloudForms のイベントに変換します。

1. AWS マネジメントコンソールで AWS Config サービスを有効化します。詳しい情報

は、『AWS Config Developer Guide』 を参照してください。

2. **AWSConfig_topic** という名前の新しい Amazon SNS トピックを作成します。Red Hat CloudForms はこのトピックに自動的に接続します。

3. (オプション) AWS マネジメントコンソールの差分作成の頻度を設定します。

Red Hat CloudForms ポリシーは、以下にリストする AWS イベントに対する割り当てることが可能です。アプライアンスは、**AWS_EC2_Instance_UPDATE** を除くこれらの全イベントでプロバイダーの更新を実行します。

イベント	ポリシー	更新
AWS_EC2_Instance_CREATE	src_vm vm_create	ems
AWS_EC2_Instance_UPDATE	該当なし	ems
AWS_EC2_Instance_running	src_vm vm_start	ems
AWS_EC2_Instance_stopped	src_vm vm_power_off	ems
AWS_EC2_Instance_shutting-down	src_vm vm_power_off	ems

3.4. GOOGLE COMPUTE ENGINE プロバイダー

3.4.1. Google Compute Engine プロバイダーの追加

初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、 以下の手順で Google Compute Engine プロバイダーを追加します。

前提条件

Google Compute Engine プロバイダーを Red Hat CloudForms に追加するための要件は以下のとおりです。

- Google Cloud Platform アカウント
- Google Compute Engine API が有効化された Google Compute Engine プロジェクト

- 対象のプロジェクトのサービスアカウント JSON キー

> **注記**
>
> 対象のプロジェクト用のプライベート JSON キーは、 Google Cloud Platform の **IAM と管理 → サービスアカウント** で生成することができます。このキーは、プロバイダーに対して認証を行う際に使用されます。
>
> 詳しい情報は、https://cloud.google.com/storage/docs/authentication で Google Cloud Platform のドキュメントを参照してください。

Google Compute Engine プロバイダーを追加する手順

1. **コンピュート → クラウド → プロバイダー** に移動します。
2. **(構成)** をクリックして **(新規クラウドプロバイダーの追加)** を選択します。
3. プロバイダーの **名前** を入力します。
4. **タイプ** の一覧から **Google Compute Engine** を選択します。
5. 一覧から **優先リージョン** を選択します。
6. **プロジェクト** から Google Compute Engine のプロジェクト ID を入力します。
7. 複数の **ゾーン** が利用可能な場合には、適切なゾーンを選択します。Red Hat は、 Google Compute Engine プロバイダー向けに新規ゾーンを作成することを推奨します。
8. 対象のプロジェクトの **サービスアカウント** JSON キーの内容を **サービスアカウント JSON** フィールドにコピーします。
9. **検証** をクリックして認証情報を検証します。
10. **追加** をクリックします。

> **注記**
>
> NTP 同期が有効になっていて、機能していることを確認してください。クロックが同期していないと、以下のエラーが発生します。
>
> **Credential validation was not successful: Authorization failed. Server message: { "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token and in a reasonable timeframe" }**

3.4.2. Google Compute Engine イベントの有効化

Google Compute Engine を Red Hat CloudForms のプロバイダーとして追加した後には、そのプロバイダーのイベントを有効化して、Red Hat CloudForms からシステムをモニタリングできるようにします。

イベントは、Google Stackdriver ロギングを Google Pub/Sub と組み合わせて使用して、プロジェクトごとに設定されます。Stackdriver ロギングは、Google のサービスおよびアプリケーションのログイベントをアグリゲートして公開するサービスです。Stackdriver はログイベントを Google

Pub/Sub のメッセージングサービスに対してエクスポートします。本項では、Google Compute Engine プロジェクトのアクティビティーログのエントリーをエクスポートして、イベントが Red Hat CloudForms でキャプチャーされるようにする方法について説明します。

Google Compute Engine イベントをエクスポートするための前提条件

- エクスポートするプロジェクトに対する所有者の権限があること。
- Google Cloud Pub/Sub API が対象のプロジェクトに対して有効化されていること。API は以下の手順で有効化します。

    1. Google Cloud Platform で、トップメニューバーから対象のプロジェクトを選択します。
    2. をクリックして **ツールとサービス** メニューを表示します。**API Manager** をクリックして https://console.cloud.google.com/apis/library/ に進みます。
    3. API Manager の **概要** タブの **Google API** 検索バーで **`Pub/Sub`** を検索し、結果から **Google Cloud Pub/Sub API** を選択します。**有効にする** のボタンをクリックします。
    4. Google Cloud Pub/Sub API がすでに有効化されている場合には、**有効にする** のボタンは表示されず、代わりに **Google Cloud Pub/Sub API** が **有効な API** の下に表示されます。

- Stackdriver ロギングサービスには、対象のプロジェクトの Pub/Sub サービスに対してパブリッシュするための権限が付与されている必要があります。必要な権限を追加するには、以下の手順に従います。

    1. Google Cloud Platform で、対象のプロジェクトを選択してから **ツールとサービス** → **IAM と管理** → **IAM** に移動して https://console.cloud.google.com/iam-admin/iam/ に進みます。
    2. **ログ設定書き込み** の権限を対象のプロジェクトに割り当てます。

        a. **`cloud-logs@system.gserviceaccount.com`** アカウントがすでに **メンバー** の下にリストされている場合には、**役割** の下に **ログ設定書き込み** が選択されていることを確認してください。

        b. **`cloud-logs@system.gserviceaccount.com`** アカウントが **メンバー** の下にリストされていない場合には、以下のステップを実行します。

            i. **追加** をクリックして権限を追加します。

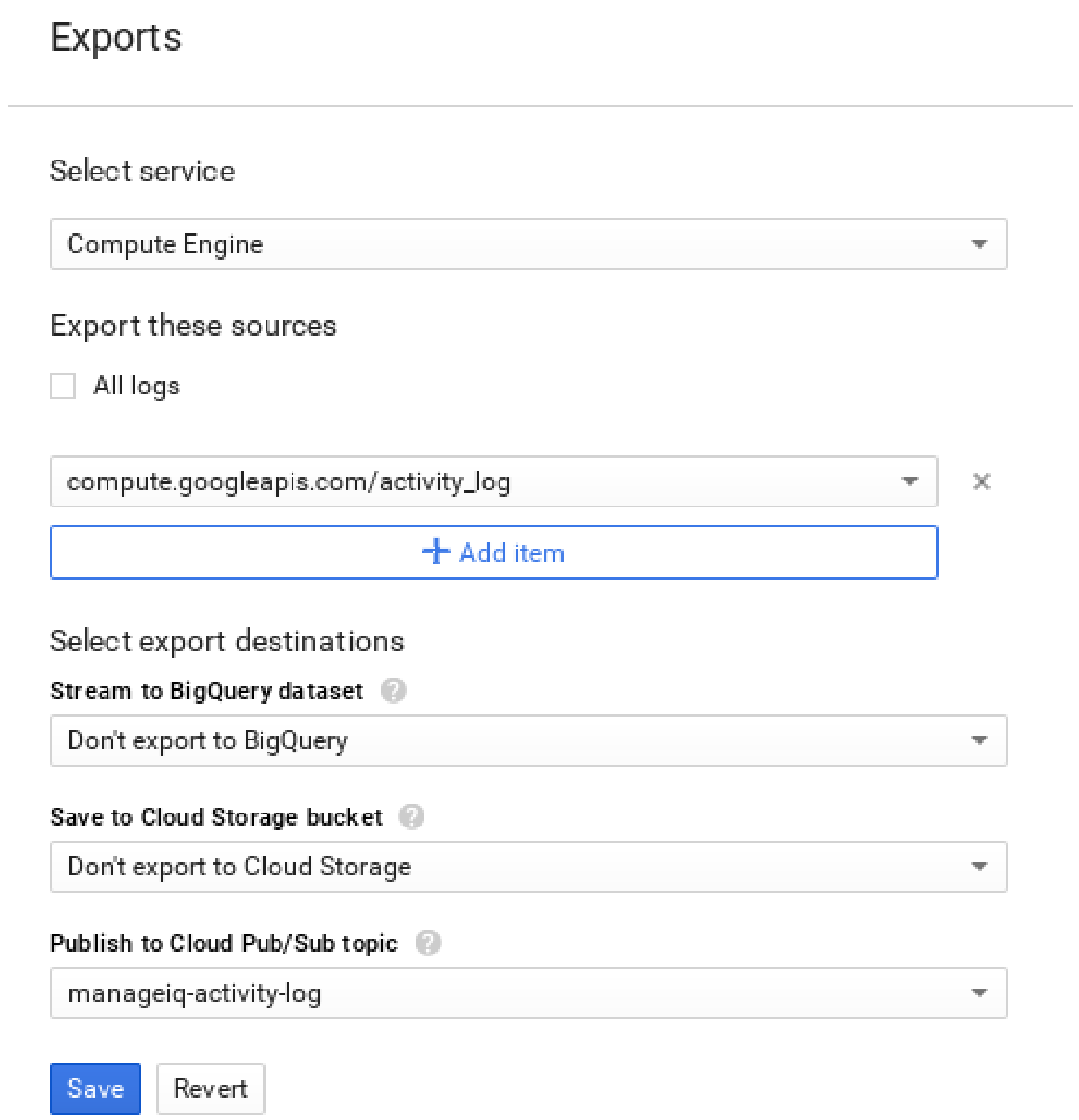
            ii. ダイアログボックスで、**メンバー** に **`cloud-logs@system.gserviceaccount.com`** を入力して Google API サービスアカウントを権限リストに追加します。

            iii. **役割を選択** のドロップダウンメニューで **ログ** → **ログ設定書き込み** の順に選択し、**追加** をクリックします。

3.4.2.1. Google Compute Engine でイベントをエクスポートするための設定

Google Compute Engine イベントをエクスポートするための前提条件のステップが完了したら、以下のステップに従って、Red Hat CloudForms にイベントをエクスポートするための Google Compute Engine プロジェクトを設定します。

1. Google Cloud Platform で、 をクリックして **ツールとサービス** メニューを表示します。**ログ** をクリックして https://console.cloud.google.com/logs/ に進みます。
2. トップメニューバーから対象のプロジェクトを選択します。
3. **ログ** メニューから **エクスポート** を選択します。
4. **サービスを選択** の一覧で、**Compute Engine** を選択します。
5. **Export these sources** で **Add item** をクリックし、一覧から **`compute.googleapis.com/activity_log`** を選択します。
6. **Select export destinations** で **Publish to Cloud Pub/Sub topic** ドロップダウンをクリックして、**Add new topic...** を選択します。
7. **Create Cloud Pub/Sub Topic** ダイアログで **Name** に **`manageiq-activity-log`** を入力します。**Create** をクリックします。



8. **保存** をクリックします。

Google Compute Engine インスタンスで変更が発生すると、Red Hat CloudForms は通知を受けて、それらの変更をイベントとして報告します。

注記

Google Compute Engine に関する更に詳しい情報は、Google Cloud Platform のドキュメントを参照してください。

- Google Cloud Platform におけるクラウドログのエクスポート設定に関する情報は、https://cloud.google.com/logging/docs/export/configure_export を参照してください。
- Google Cloud Pub/Sub API の運用とコストに関する情報は、https://cloud.google.com/pubsub/ を参照してください。

3.4.2.2. Red Hat CloudForms での Google Compute Engine イベントの表示

Red Hat CloudForms で以下の手順に従って Google Compute Engine プロジェクトのイベントを表示します。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動して対象の Google Compute Engine プロジェクトを選択します。
2. プロバイダーの概要ページで **監視** → **タイムライン** をクリックして、そのプロジェクトのイベントタイムラインを表示します。

3.5. クラウドプロバイダーの更新

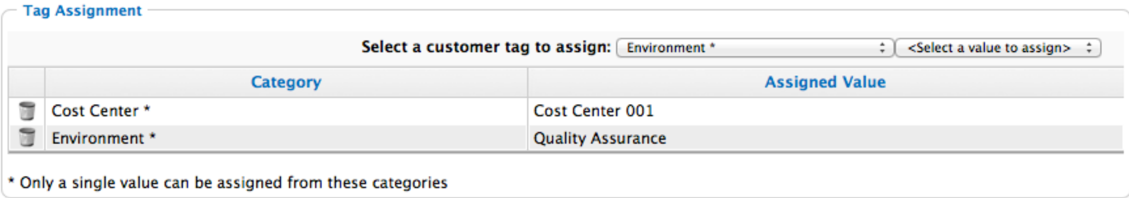
クラウドプロバイダーを更新して、関連するその他のリソースを確認します。選択したクラウドプロバイダーの正しい認証情報があることを確認してから、更新を実行してください。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。
2. クラウドプロバイダーのチェックボックスを選択して更新します。
3. (**構成**) をクリックして、 (**リレーションシップと電源状態の更新**) を選択します。
4. **OK** をクリックします。

3.6. クラウドプロバイダーのタグ付け

同時にまとめて分類するには、全クラウドプロバイダーにタグを適用します。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。
2. タグ付けするクラウドプロバイダーのチェックボックスを選択します。
3. (**ポリシー**) をクリックして、 (**タグの編集**) を選択します。
4. 最初の一覧から割り当てるカスタマータグを選択します。



5. 2 番目のリストから割り当てる値を選択します。

6. **保存** をクリックします。

3.7. クラウドプロバイダーの削除

使用しなくなったクラウドプロバイダーを VMDB から削除する必要がある場合があります。

1. **コンピュート → クラウド → プロバイダー** に移動します。

2. 削除するクラウドプロバイダーにチェックを付けます。

3. **(構成)** をクリックして、 **(VMDB からのクラウドプロバイダーの削除)** を選択します。

4. **OK** をクリックします。

3.8. クラウドプロバイダーの編集

プロバイダーの情報 (例: 名前、IP アドレス、ログイン認証情報) を編集します。

注記

タイプ の値は変更できません。

異なるクラウドプロバイダーを使用するには、新規作成します。

1. **コンピュート → クラウド → プロバイダー** に移動します。

2. 編集するクラウドプロバイダーをクリックします。

3. **(構成)** をクリックして、 **(選択したクラウドプロバイダーの編集)** を選択します。

4. **基本情報** を編集します。表示される項目は、プロバイダーの ***タイプ*** によって異なります。

5. **認証情報** のセクションで **ユーザー名** と **パスワード** を入力してから、**パスワードの確認** で確認のためにパスワードを再入力します。

   - **Amazon EC2** を選択する場合には、Amazon AWS アカウントの **セキュリティ認証情報** で **アクセスキー** を生成します。**アクセスキー ID** は **ユーザー ID** として機能し、**シークレットアクセスキー** は **パスワード** として機能します。

   - **OpenStack** を選択する場合には、ログイン認証情報に **`Keystone` のユーザー `ID`** と **パスワード** を使用します。

6. OpenStack プロバイダーを編集する場合には、**AMQP** サブタブを使用して、OpenStack Nova コンポーネントの Advanced Message Queuing Protocol サービスに必要な認証情報を入力します。

7. **検証** をクリックして、検証が成功したことを知らせるメッセージが表示されるのを待ちます。

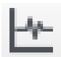
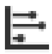
8. **保存** をクリックします。

3.9. クラウドプロバイダーのタイムラインの表示

クラウドプロバイダーに登録されているインスタンスのイベントのタイムラインを表示します。

1. **コンピュート** → **クラウド** → **プロバイダー** に移動します。

2. タイムラインを表示するクラウドプロバイダーをクリックします。

3.  **(監視)** をクリックして、  **(タイムライン)** を選択します。

4. **オプション** から、表示する期間や表示するイベントタイプをカスタマイズします。

   - **表示** を使用して、通常の管理イベントとポリシーイベントを選択します。
   - **タイプ** の一覧で毎時または毎日のデータポイントを選択します。
   - **日付** で、表示するタイムラインの日付を入力します。
   - 毎日のタイムラインを表示するように選択した場合は、**表示** を使用して、何日分遡るかを設定します。最大の履歴は 31 日です。
   - 3 つの **イベントグループ** リストでは、異なるイベントグループを選択して表示することができます。それぞれ独自の色が使用されます。
   - **レベル** の一覧で **概要** のイベントか、イベントの **詳細** の一覧を選択します。

第4章 ネットワークプロバイダー

Red Hat CloudForms には、**ネットワークマネージャー** と呼ばれる新たなプロバイダータイプが導入されました。この新しいプロバイダータイプは、**OpenStack Network (Neutron)**、**Azure ネットワーク**、**Amazon EC2 ネットワーク** をはじめとするソフトウェア定義ネットワーク (SDN) プロバイダーを公開します。SDN インベントリーコレクションは OpenStack、Amazon、Azure プロバイダーに対して有効化されています。OpenStack Network プロバイダーは、毎回 OpenStack のデータベースにクエリーを実行せずに IP を割り当てられるようにするために、OpenStack から Floating IP のインベントリーを収集します。また、OpenStack および OpenStack インフラストラクチャーから Neutron の全データを更新し、Neutron のロジックを共通の場所に抽出します。ネットワークプロバイダー設定の管理は現在無効になっている点に注意してください。

4.1. ネットワークプロバイダーの追加/表示

注記

クラウドプロバイダーを追加/削除すると、そのプロバイダーに対応するサポート対象のネットワークプロバイダー (OpenStack Network、Azure ネットワーク、Amazon EC2 ネットワーク) はすべて、自動的に追加/削除されます。

ネットワークプロバイダーの表示

1. **ネットワーク** → **プロバイダー** に移動すると、全ネットワークプロバイダーの一覧が **名前**、**タイプ**、**EVM ゾーン**、**インスタンス数**、 **サブネット**、**リージョン** とともに表示されます。

2. この一覧からプロバイダーをクリックすると、概要の画面が表示されます。

ネットワークプロバイダーの概要:

概要画面には、以下の情報を含むテーブルが表示されます。**プロパティー**、**ステータス**、**リレーションシップ**、**概要**、および **スマート管理**。**リレーションシップ** と **概要** テーブルの行をクリックすると、個別エンティティーの詳細情報が表示されます。

サイドバーにあるアコーディオンタブからは **プロパティー** と **リレーションシップ** の詳細にアクセスできます。

タスクバーにある **リロード**、**構成**、**ポリシー**、**監視** のボタンでプロバイダーを管理します。

注記

または、クラウドプロバイダーを 1 つクリックすると、そのクラウドプロバイダーの詳細情報とネットワークマネージャー、テナント、インスタンスおよびその他のリレーションシップが表示されます。リレーションシップでネットワークマネージャーをクリックすると、ネットワークプロバイダーの情報と、そのプロバイダーとクラウドプロバイダーのリレーションシップが概要ページに表示されます。

4.2. ネットワークプロバイダーの更新

ネットワークプロバイダーを更新して、そのプロバイダーに関連するその他のリソースを確認します。更新を行う前には、選択したプロバイダーに正しい認証情報があることを確認してください。

1. **ネットワーク** → **プロバイダー** に移動します。
2. 更新するネットワークプロバイダーを選択します。
3. (**構成**) をクリックして、 (**リレーションシップと電源状態の更新**) を選択します。
4. **OK** をクリックします。

4.3. ネットワークプロバイダーのタグ付け

ネットワークプロバイダーを同時にまとめて分類するには、タグを適用します。

1. **ネットワーク** → **プロバイダー** に移動します。
2. タグ付けするネットワークプロバイダーを選択します。
3. (**ポリシー**) をクリックして、 (**タグの編集**) を選択します。
4. **割り当てるカスタマータグの選択** をクリックします。
5. 2 番目のリストから割り当てる値を選択します。
6. **保存** をクリックします。

4.4. ネットワークプロバイダーの削除

クラウドプロバイダーを追加/削除すると、そのプロバイダーに対応するネットワークプロバイダーは自動的に追加/削除されますが、使用しなくなったネットワークプロバイダーを手動で削除することも可能です。この操作を実行すると、そのネットワークプロバイダーは VMDB およびクラウドプロバイダーのリレーションシップから削除されます。

1. **ネットワーク** → **プロバイダー** に移動します。
2. 削除するネットワークプロバイダーをクリックします。
3. (**構成**) をクリックして、 (**このネットワークプロバイダーを VMDB から削除する**) を選択します。
4. **OK** をクリックします。

4.5. ネットワークプロバイダーのタイムラインの表示

ネットワークプロバイダーに登録されているインスタンスのイベントのタイムラインを表示します。

1. **ネットワーク** → **プロバイダー** に移動します。
2. タイムラインを監視するネットワークプロバイダーをクリックします。
3. (**監視**) をクリックして、 (**タイムライン**) を選択します。
4. **オプション** から、イベントタイプと間隔を選択し、表示する期間や表示するイベントタイ

プをカスタマイズします。

- **表示** の一覧から、**管理イベント** または **ポリシーイベント** を選択します。
- **間隔** には **毎時** または **毎日** を選択します。
- **日付** を選択します。
- **間隔** に **毎日** を選択した場合には、イベントのタイムラインの表示で遡る期間を日数で設定します。最大は **31 日前** です。
- **レベル** には **概要** または **詳細** を選択します。
- タイムラインを監視する、必要な **イベントグループ** を一覧から選択します。

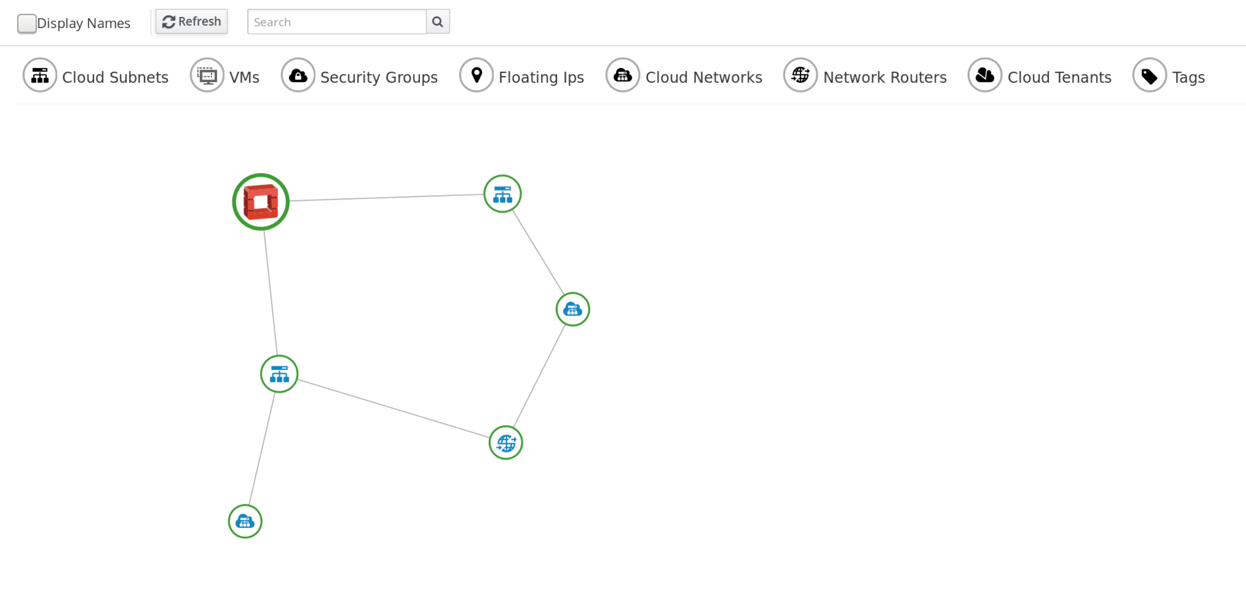
ネットワークプロバイダーにポリシープロファイルを割り当て/削除することができます。その手順は、通常のポリシープロファイルの場合と同様です。**『Policies and Profiles Guide』**の「Assigning Policy Profiles to a Network Provider」および「Removing Policy Profiles from a Network Provider」を参照してください。

4.6. ネットワークプロバイダーでのトポロジーウィジェットの使用

トポロジー ウィジェットは、Red Hat CloudForms がアクセス可能なネットワークプロバイダーの異なるエンティティー間のステータスとリレーションシップを表示する、インタラクティブなトポロジーグラフです。

トポロジーグラフには、ネットワークのプロバイダー環境全体内のクラウドサブネット、仮想マシン、セキュリティーグループ、Floating IP アドレス、クラウドネットワーク、ネットワークルーター、クラウドテナント、およびタグが含まれます。

グラフ内の各エンティティーはステータスが色別で表示され、緑はアクティブ、赤が非アクティブもしくは問題ありを示します。



トポロジーウィジェットの使用

1. **ネットワーク** → **トポロジー** に移動します。
2. プロバイダーの概要を表示するネットワークプロバイダーをクリックします。

別の方法では、プロバイダーの概要ページにある **概要** のボックスで **トポロジー** をクリックする

と、トポロジーウィジェットが開きます。

- グラフの各要素の上にマウスを移動すると、その要素の情報の概要が表示されます。
- グラフ内のエンティティーをダブルクリックすると、それらの概要ページに移動します。
- 要素をドラッグするとグラフの配置を変更することができます。
- エンティティーの表示/非表示を切り替えるには、グラフの最上部の凡例をクリックします。
- エンティティーの名前の表示/非表示を切り替えるには、**名前の表示** チェックボックスをクリックします。
- ネットワークプロバイダーエンティティーの表示を更新するには、**更新** ボタンをクリックします。
- エンティティーを名前で検索するには、**検索** ボックスに名前の一部またはすべてを入力します。

第5章 ミドルウェアプロバイダー

Red Hat CloudForms におけるミドルウェアプロバイダーとは、 Red Hat CloudForms アプライアンスを追加して環境内のリソースの管理やそれらのリソースとの対話を行うことができるミドルウェア管理環境のことを指します。本章では、Red Hat CloudForms に追加可能なミドルウェアプロバイダーの異なるタイプとそれらの管理方法について説明します。

5.1. ミドルウェアの管理

ミドルウェアプロバイダーは、Red Hat CloudForms の管理機能を、管理仮想マシン、ホスト、および Linux コンテナーで実行中の JBoss Middleware アプリケーションコンテナーに拡張します。プロバイダーは、インベントリー、イベント、メトリック、および電源操作を提供します。Red Hat CloudForms のミドルウェア管理は、Hawkular オープンソースプロジェクトを基にしたプロバイダーです。機能が完全な場合は、このミドルウェア管理プロバイダーは現在の Red Hat ミドルウェア管理オファリングである JBoss Operations Network に代わるものになります。

注記

ミドルウェア管理プロバイダーは、Red Hat CloudForms の本リリースではテクノロジープレビューとして提供されています。テクノロジープレビューとされている機能のサポート範囲に関する情報は、「テクノロジプレビュー機能のサポート範囲」を参照してください。

5.1.1. ミドルウェア管理プロバイダーの追加

ミドルウェア管理プロバイダーを追加するには、以下の手順に従います。

1. **ミドルウェア** → **プロバイダー** に移動します。
2. (**構成**) をクリックして (**新規ミドルウェアプロバイダーの追加**) を選択します。
3. 新規ミドルウェアプロバイダーの追加画面で以下を入力します。
   - **名前** に Middleware Manager などのプロバイダーの名前を入力します。
   - **タイプ** の一覧から **Hawkular** を選択します。
   - **ゾーン** はデフォルトのゾーンにしておきます。

   エンドポイント

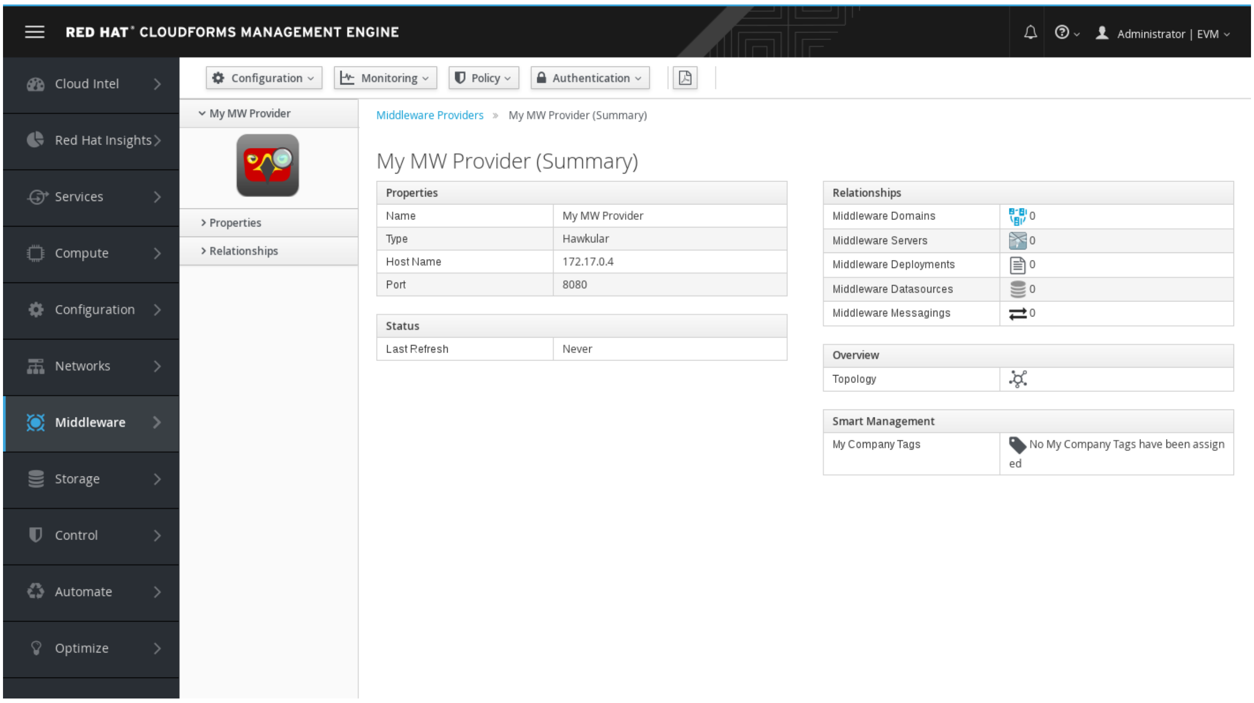
   - **ホスト名 (または IPv4 または IPv6 アドレス)** には、ミドルウェアマネージャーをインストールしたマシンのホスト名を入力します。
   - **API ポート** には、ミドルウェアマネージャーのポートを入力します。デフォルトでは、8080 を使用します。
   - **ユーザー名** には、ミドルウェアマネージャーの起動に使用するユーザー名を指定します。これは、**`HAWKULAR_USERNAME`** と一致するようにしてください。
   - **パスワード** には、**`HAWKULAR_PASSWORD`** と一致するパスワードを入力します。
   - **パスワードの確認** には、パスワードを再入力します。

4. プロバイダーを追加する前に、**検証** ボタンをクリックしてユーザーに適切な資格があることを確認します。

5. **追加** をクリックします。

6. **(構成)** をクリックしてから、 **(項目とリレーションシップの更新)** をクリックします。

Red Hat CloudForms で概要画面が表示されます。



第6章 コンテナープロバイダー

コンテナープロバイダーとは、コンテナーのリソースを管理するサービスで、 Red Hat CloudForms アプライアンスに追加することができます。

コンピュート → **コンテナー** のセクションには、コンテナープロバイダーを追加および管理するためのオプションがあります。これには、検出/追加されたコンテナープロバイダーをすべて表示する **プロバイダー** ページが含まれます。

Red Hat CloudForms は、コンテナープロバイダーとして OpenShift Enterprise の追加をサポートしています。

6.1. OPENSHIFT ENTERPRISE MANAGEMENT トークンの取得

`openshift-ansible-3.0.20` (またはそれ以降のバージョン) を使用して OpenShift Enterprise をデプロイする場合には、Red Hat CloudForms で必要なサービスアカウントとロールはデフォルトでインストールされます。

プロバイダーの定義に使用するトークンを取得するには、以下の手順で、お使いの OpenShift Enterprise のバージョンに対応するステップに従ってください。

6.1.1. OpenShift Enterprise 3.2 の管理トークンの取得

ターミナルを開いて、以下のコマンドを実行します。

```
# oc sa get-token -n management-infra management-admin
eyJhbGciOiJSUzI1NiI...
```

このコマンドは、OpenShift Enterprise プロバイダーを追加するのに必要なトークンを提供します。

6.1.2. OpenShift Enterprise 3.1 の管理トークンの取得

ターミナルを開いて、以下の手順を実行します。

1. **`management`** サービスアカウントのトークン名を取得するには、以下のコマンドを実行します。

   ```
   # oc describe sa -n management-infra management-admin
   ...
   Tokens:  management-admin-token-0f3fh
            management-admin-token-q7a87
   ```

2. トークンを 1 つ選択して以下のコマンドを実行し、トークンの完全な出力を取得します。

   ```
   # oc describe secret -n management-infra management-admin-token-
   0f3fh
   ...
   Data
   ====
   token:  eyJhbGciOiJSUzI1NiI...
   ```

management-admin-token-0f3fh は、実際のトークンの名前に置き換えます。

このコマンドは、OpenShift Enterprise プロバイダーを追加するのに必要なトークンを提供します。

6.2. OPENSHIFT メトリックの設定

ノード、ポッド、コンテナーのメトリックを収集するには、クラスター内で OpenShift Metrics サービスを実行する必要があります。詳しくは、OpenShift Enterprise **『Installation and Configuration』**の「Enabling Cluster Metrics」のセクションを参照してください。

注記

メトリック収集が正常に機能するには、Red Hat CloudForms で 3 つの **容量 & 使用状況** サーバーロールすべてを利用可能にする必要があります。これは、設定メニューの **構成** → **サーバー** → **サーバー制御** で設定することができます。容量と使用状況のメトリック収集についての詳しい情報は、**『Deployment Planning Guide』**の「Assigning the Capacity and Utilization Server Roles」のセクションを参照してください。

6.3. OPENSHIFT ENTERPRISE プロバイダーの追加

初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、「OpenShift Enterprise Management トークンの取得」で取得したトークンを使用して OpenShift Enterprise プロバイダーを追加し、以下の手順を実行します。

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. (**構成**) をクリックして、 (**新規コンテナープロバイダーの追加**) を選択します。
3. プロバイダーの **名前** を入力します。
4. **タイプ** の一覧から **OpenShift Enterprise** を選択します。
5. プロバイダー用に適切な **ゾーン** を入力します。デフォルトでは、ゾーンは **default** に設定されます。
6. プロバイダーの **ホスト名または IP アドレス** を入力します。

   重要

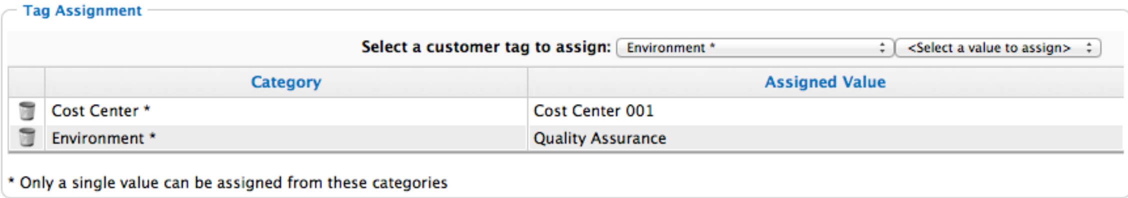
   ホスト名 には、完全修飾ドメイン名を使用する必要があります。

7. プロバイダーの **ポート** を入力します。デフォルトのポートは **8443** です。
8. **認証情報** のセクションで、**トークン** フィールドにトークンを入力します。このトークンは、「OpenShift Enterprise Management トークンの取得」で事前に取得済みのトークンです。
   - **検証** をクリックして、Red Hat CloudForms が指定したトークンで OpenShift Enterprise プロバイダーに接続できることを確認します。
9. **追加** をクリックします。

6.4. コンテナープロバイダーのタグ付け

ネットワークプロバイダーを同時にまとめて分類するには、タグを適用します。

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. タグ付けするコンテナープロバイダーのチェックボックスを選択します。
3.  (**ポリシー**) をクリックして、  (**タグの編集**) を選択します。
4. ドロップダウンメニューから割り当てるタグを選択します。



5. 割り当てる値を選択します。
6. **保存** をクリックします。

6.5. コンテナープロバイダーの削除

使用しなくなったコンテナープロバイダーは VMDB から削除する必要がある場合があります。

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. 削除するコンテナープロバイダーのチェックボックスを選択します。
3.  (**構成**) をクリックして、  (**VMDB からコンテナープロバイダーの削除**) を選択します。
4. **OK** をクリックします。

6.6. コンテナープロバイダーの編集

プロバイダーの情報 (例: 名前、ホスト名、IP アドレス、ポート) を編集します。

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. 編集するコンテナープロバイダーをクリックします。
3.  (**構成**) をクリックして、  (**選択したコンテナープロバイダーの編集**) を選択します。
4. **基本情報** を編集します。表示される項目は、プロバイダーの **タイプ** によって異なります。

> **注記**
>
> **タイプ** の値は変更できません。

異なるコンテナープロバイダーを使用するには、新規作成します。

5. 新しい **トークン** 入力して **認証情報** を編集します。
6. **検証** をクリックして、検証が成功したことを知らせるメッセージが表示されるのを待ちます。
7. **保存** をクリックします。

6.7. コンテナープロバイダーのタイムラインの表示

コンテナープロバイダーに登録されているインスタンスのイベントのタイムラインを表示します。

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. タイムラインを表示するコンテナープロバイダーをクリックします。
3. (**監視**) をクリックして、 (**タイムライン**) を選択します。
4. **オプション** から、表示する期間や表示するイベントタイプをカスタマイズします。
   - **表示** を使用して、通常の管理イベントとポリシーイベントを選択します。
   - **間隔** のドロップダウンを使用して、毎時または毎日のいずれかのデータポイントを選択します。
   - **日付** で、表示するタイムラインの日付を入力します。
   - 毎日のタイムラインを表示するように選択した場合は、**表示** を使用して、何日分遡るかを設定します。最大の履歴は 31 日です。
   - **レベル** のドロップダウンリストで **概要** のイベントか、イベントの **詳細** の一覧を選択します。
   - 3 つの **イベントグループ** ドロップダウンリストでは、異なるイベントグループを選択して表示することができます。それぞれ独自の色が使用されます。

タイムラインでアイテムの詳細を確認するには、そのアイテムをクリックします。リソースへのリンクが吹き出しに表示されます。

6.8. インサイトと制御

Red Hat CloudForms は、OpenShift Enterprise コンテナープロバイダーに接続してそれらのプロバイダーを管理することができます。これは、インフラストラクチャーおよびクラウドのプロバイダーを管理するのと同様です。これにより、環境のさまざまな側面を制御し、以下のような情報を確認することが可能となります。

- 環境内のコンテナー数
- 特定のノードに十分なリソースがあるかどうか

- 使用されている個別のイメージ数
- 使用されているイメージレジストリー

Red Hat CloudForms は、コンテナー環境に接続する際に、環境の異なる領域の情報を収集します。

- ポッド、ノード、サービスなどのエンティティー
- エンティティー間の基本的なリレーションシップ (例: ポッドに対してサービスを提供しているサービス)
- リレーションシップに関する詳細なインサイト (例: 同じイメージを使用している 2 つのコンテナー)
- イベント、プロジェクト、ルート、メトリックなどの追加情報

タグを追加することによってコンテナーのエンティティーのポリシーを管理することができます。ボリューム以外のコンテナーエンティティーはすべてタグ付けすることが可能です。

6.8.1. プロバイダー間共通のインサイト

プロバイダー間共通のインサイトは、Red Hat CloudForms が認識しているインフラストラクチャーの全レイヤーを結び付けて、分析のためのデータを収集する機能です。

この機能は、以下の環境内で利用可能な全レイヤーのクロスリンクをサポートしています。

- OpenStack
- Red Hat Enterprise Virtualization
- VMware vCenter
- Amazon EC2
- Google Cloud Engine

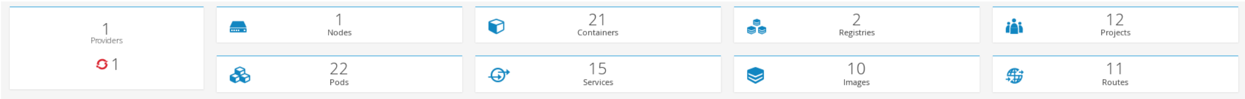
収集される情報には、その他 (インフラストラクチャーまたはクラウド) のプロバイダーで利用可能な全データも含まれます。

注記

Amazon EC2 (AWS) および Google Cloud Engine (GCE) をサポートするには、適切なクラウドプロバイダーを使用して OpenShift をインストールする必要があります。詳しくは、『OpenShift Enterprise Installation and Configuration』ガイドを参照してください。

6.8.2. コンテナーの概要のページを使用した作業

Red Hat CloudForms が認識している全コンテナープロバイダーおよびエンティティーについての情報は、コンテナーの **概要** ページに要約されます。**概要** のページでは、コンテナープロバイダーおよびエンティティーについてのさらに詳しい情報を記載した他の概要ページへのリンクが提供されます。**概要** ページでは、**集計されたノードの使用状況**、**ネットワーク使用状況のトレンド**、**新規イメージ使用状況のトレンド**、**ノードの使用状況**、および **ポッド作成および削除のトレンド** についてのメトリックが表示されます。



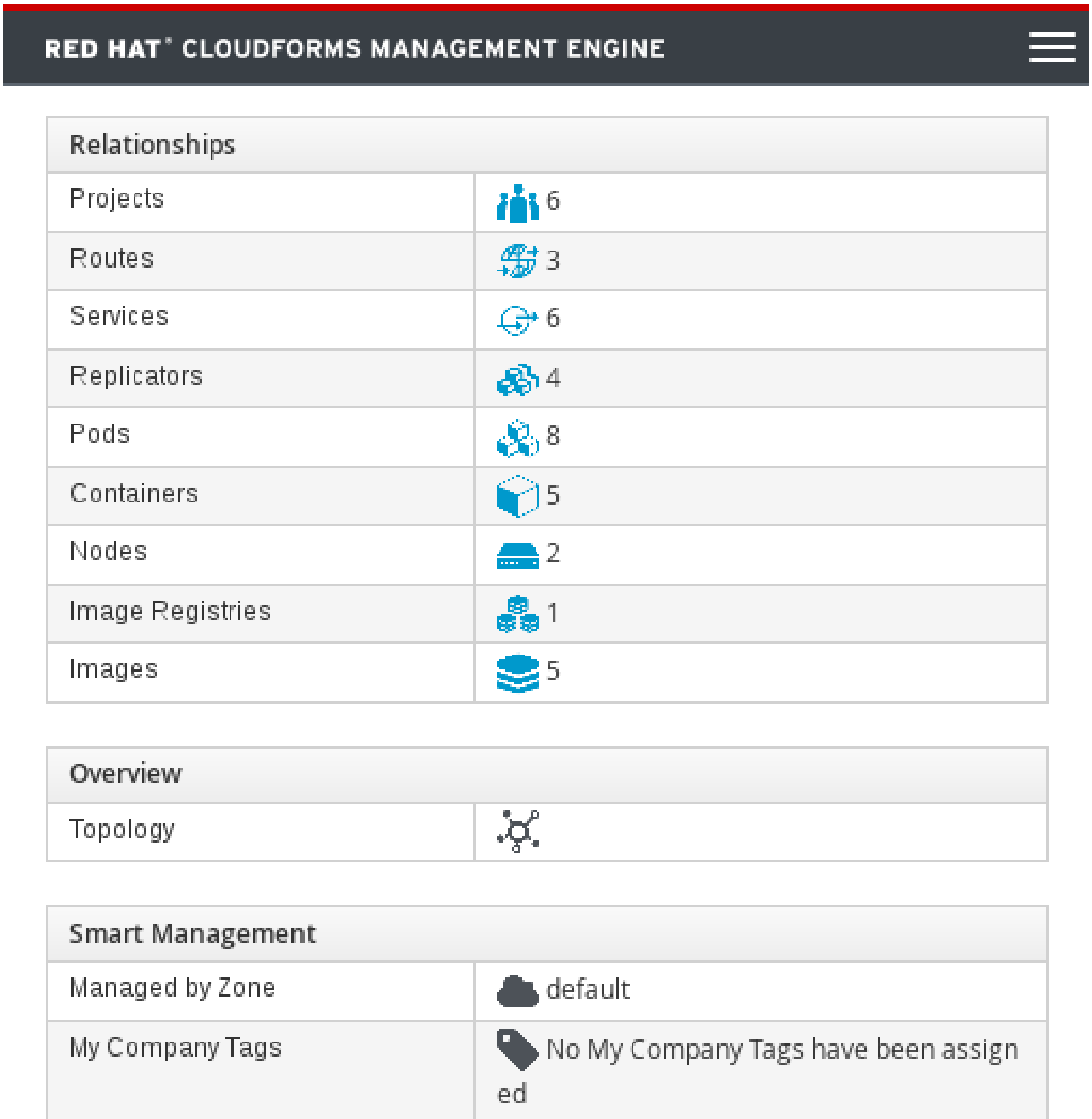
コンテナーの概要のページを使用した作業

1. **コンピュート** → **コンテナー** → **概要** に移動します。
2. 必要なコンテナーのエンティティーまたはプロバイダー (該当する場合) をクリックして、概要とさらなる情報を表示します。

6.8.3. コンテナープロバイダーの概要の表示

コンテナープロバイダー の概要ページでは、コンテナープロバイダーのさまざまな側面の情報を確認することができます。以下に例を示します。

- プロバイダーとそのコンポーネントのステータス
- コンテナープロバイダーの異なるエンティティー間のリレーションシップ。これらのリレーションシップは、概要ページの右側の **リレーションシップ** のボックスに要約されます。



- 全ノードの全 CPU コアの総容量および全ノードの全メモリーの総容量についての追加情報

コンテナープロバイダーの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。

6.8.4. コンテナーノードの概要の表示

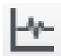
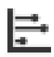
コンテナーノード の概要ページでは、コンテナーノードのさまざまな側面の情報を確認することができます。以下に例を示します。

- ノード上のエンティティーの数
- 容量と使用状況
- ベースに使用されているオペレーティングシステムとソフトウェアのバージョン

コンテナーノードの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**ノード** をクリックします。
4. 必要なコンテナーノードをクリックして表示します。
5. または、**コンピュート** → **コンテナー** → **コンテナーノード** から必要なコンテナーノードにアクセスすることができます。

6.8.4.1. コンテナーノードのタイムラインの表示

ノードのイベントのタイムラインを確認することができます。コンテナーノードの概要ページからタイムラインにアクセスするには、 **(監視)** をクリックして、 **(タイムライン)** 選択します。

6.8.5. コンテナーの概要の表示

コンテナー の概要ページでは、コンテナーのさまざまな側面の情報を確認することができます。以下に例を示します。

- コンテナーと関連するノード/ポッド/イメージとの関係
- コンテナーが実行されているノード
- コンテナーとなっているポッドの部分
- コンテナーの ID
- コンテナーイメージの名前およびその他のプロパティー (例: タグ)

コンテナーの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。

2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。

3. 概要のページの右側にある **リレーションシップ** のボックスで、**コンテナー** をクリックします。

4. 必要なコンテナーをクリックして表示します。

5. または、**コンピュート** → **コンテナー** → **コンテナー** から必要なコンテナーにアクセスすることができます。

6.8.6. コンテナーイメージの概要の表示

コンテナーイメージ の概要ページでは、コンテナーイメージのさまざまな側面の情報を確認することができます。以下に例を示します。

- イメージを使用しているコンテナー
- イメージの元のイメージレジストリー

コンテナーイメージの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。

2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。

3. 概要のページの右側にある **リレーションシップ** のボックスで、**イメージ** をクリックします。

4. 必要なイメージをクリックして表示します。

5. または、**コンピュート** → **コンテナー** → **コンテナーイメージ** から必要なイメージにアクセスすることができます。

6.8.7. イメージレジストリーの概要の表示

イメージレジストリー の概要ページでは、イメージレジストリーのさまざまな側面の情報を確認することができます。以下に例を示します。

- そのレジストリーから使用されているイメージとその数
- そのレジストリーからイメージを使用しているコンテナー
- レジストリーのホストとポート

イメージレジストリーの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。

2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。

3. 概要のページの右側にある **リレーションシップ** のボックスで、**イメージレジストリー** をクリックします。

4. 必要なイメージレジストリーをクリックして表示します

5. または、**コンピュート** → **コンテナー** → **コンテナーレジストリー** から必要なイメージレジストリーにアクセスすることができます。

6.8.8. ポッドの概要の表示

ポッド の概要ページでは、ポッドのさまざまな側面の情報を確認することができます。以下に例を示します。

- そのポッドに属するコンテナー
- そのポッドを参照するサービス
- ポッドを実行しているノード
- ポッドがレプリケーターで制御されているかどうか
- ポッドの IP アドレス

ポッドの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**ポッド** をクリックします。
4. 必要なポッドをクリックして表示します。
5. または、**コンピュート** → **コンテナー** → **ポッド** から必要なポッドにアクセスすることができます。

6.8.9. レプリケーターの概要の表示

レプリケーター の概要ページでは、レプリケーターのさまざまな側面の情報を確認することができます。以下に例を示します。

- 要求されたポッドの数
- 現在のポッド数
- レプリケーターのラベルとセレクター

レプリケーターの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**レプリケーター** をクリックします。
4. 必要なレプリケーターをクリックして表示します。
5. または、**コンピュート** → **コンテナー** → **レプリケーター** から必要なレプリケーターにアクセスすることができます。

6.8.10. コンテナーサービスの概要の表示

コンテナーサービス の概要ページでは、コンテナーサービスのさまざまな側面の情報を確認することができます。以下に例を示します。

- コンテナーサービスがトラフィックを提供するポッド
- コンテナーサービスのポート設定
- コンテナーサービスのラベルとセレクター

コンテナーサービスの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**サービス** をクリックします。
4. 必要なサービスをクリックして表示します。
5. または、**コンピュート** → **コンテナー** → **コンテナーサービス** から必要なサービスにアクセスすることができます。

6.8.11. ボリュームの概要の表示

ボリューム の概要ページでは、コンテナープロバイダーの永続ボリュームに関する情報を確認することができます。以下に例を示します。

- ボリュームの接続先のポッド
- ボリュームの接続パラメーター
- ボリュームのストレージ容量
- ボリュームの iSCSI ターゲットの情報 (該当する場合)

ボリュームの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**ボリューム** をクリックします。
4. 概要を表示するボリュームをクリックします。
5. 別の方法では、**コンピュート** → **コンテナー** → **ボリューム** からボリュームにアクセスすることもできます。

6.8.12. コンテナービルドの概要の表示

コンテナービルド の概要ページでは、コンテナービルドのさまざまな側面の情報を確認することができます。以下に例を示します。

- そのコンテナービルドがベースとしているビルド設定
- 作成済みのビルドインスタンス
- インスタンスが完了済みのビルドプロセス段階

- ビルドインスタンスが属するポッド

コンテナービルドの概要の表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**コンテナービルド** をクリックします。
4. 概要を表示するコンテナービルドをクリックします。
5. または、**コンテナー** → **コンテナービルド** から必要なコンテナーにアクセスすることができます。

6.8.13. コンテナーテンプレートの概要表示

コンテナーテンプレート の概要ページでは、コンテナーテンプレートのさまざまな側面の情報を確認することができます。以下に例を示します。

- テンプレートに関連付けられたプロジェクト
- テンプレートに含まれるオブジェクト
- テンプレートのオブジェクトで使用可能なパラメーター
- テンプレートのバージョン番号

コンテナーテンプレートの概要表示

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. 概要のページの右側にある **リレーションシップ** のボックスで、**コンテナーテンプレート** をクリックします。
4. 概要を表示するコンテナーテンプレートをクリックします。

または、**コンテナー** → **コンテナーテンプレート** からコンテナーテンプレート一覧にアクセスすることができます。確認するテンプレートをクリックします。

6.8.14. トポロジーウィジェットの使用

トポロジー ウィジェットは、Red Hat CloudForms がアクセス可能なコンテナープロバイダーの異なるエンティティー間のステータスとリレーションシップを表示する、インタラクティブなトポロジーグラフです。

- トポロジーグラフには、全コンテナーのプロバイダー環境内のポッド、コンテナー、サービス、ノード、仮想マシン、ホスト、ルート、レプリケーターが含まれます。
- グラフ内の各エンティティーには各ステータスが色別で表示されます。
- グラフの各要素の上にマウスを移動すると、その要素の情報の概要が表示されます。
- グラフ内のエンティティーをダブルクリックすると、それらの概要のページに移動します。

- 要素をドラッグしてグラフの配置を変更することが可能です。
- エンティティーの表示/非表示を切り替えるには、グラフの最上部の凡例をクリックします。
- エンティティーの名前の表示/非表示を切り替えるには、ページの右側の **名前の表示** をクリックします。

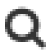
トポロジーウィジェットの使用

1. **コンピュート** → **コンテナー** → **プロバイダー** に移動します。
2. プロバイダーの概要を表示する必要なコンテナープロバイダーをクリックします。
3. プロバイダーの概要ページの右側にある **概要** のボックスで **トポロジー** をクリックします。

6.8.15. SmartState 分析の実行

コンテナーイメージの SmartState 分析を実行して、イメージに含まれるパッケージを検査します。

SmartState 分析の実行

1. **コンピュート** → **コンテナー** → **コンテナーイメージ** に移動します。
2. 分析するコンテナーイメージにチェックを付けます。複数のイメージにチェックを付けることが可能です。
3.  (**構成**) をクリックして  (**SmartState 分析の実施**) を選択します。

コンテナーイメージがスキャンされます。このプロセスにより、イメージの必要なファイルがコピーされます。イメージのページが再読み込みされた後には、新しいパッケージおよび更新されたパッケージがすべて一覧表示されます。

コンテナーイメージの SmartState Analysis タスクをモニタリングするには、設定メニューの **タスク** に移動します。開始時刻、終了時刻、タスクの現在実行中の箇所、発生したエラーなどを含む各タスクのステータスが表示されます。

第7章 ストレージマネージャー

Red Hat CloudForms におけるストレージマネージャーとは、Red Hat CloudForms アプライアンスから管理可能なストレージリソースを提供するサービスのことです。本章では、Red Hat CloudForms で使用するストレージマネージャーの異なるタイプとそれらの管理方法について説明します。

現在 Red Hat CloudForms で利用可能なストレージマネージャーは、OpenStack Block Storage (**`openstack-cinder`**) と OpenStack Object Storage (**`openstack-swift`**) の 2 つのタイプがあります。OpenStack Block Storage はブロックストレージのプロビジョニングと管理を行い、OpenStack Object Storage はクラウド内のオブジェクトストレージを管理します。これらのストレージマネージャーは、OpenStack クラウドプロバイダーの追加後に Red Hat CloudForms が自動検出します。

7.1. OPENSTACK BLOCK STORAGE MANAGERS

OpenStack Block Storage サービス (**`openstack-cinder`**) は、OpenStack インフラストラクチャーインスタンスが消費することのできる永続的なブロックストレージを提供、管理します。

OpenStack Block Storage をストレージマネージャーとして使用するには、まず OpenStack クラウドプロバイダーを Red Hat CloudForms アプライアンスに追加して、イベントを有効にする必要があります。 CloudForms が自動的に Block Storage サービスを発見し、Red Hat CloudForms 内の **Storage Managers** リストに追加します。クラウドプロバイダーの追加とイベントの有効化については、「OpenStack プロバイダーの追加」 を参照してください。

7.1.1. OpenStack Block Storage Manager でのボリューム作成

ボリュームを作成して、OpenStack Block Storage マネージャーに割り当てることができます。

以下の方法でボリュームを作成します。

1. **ストレージ** → **ボリューム** に移動します。
2. (**構成**) をクリックして、 (**新規クラウドボリュームの追加**) をクリックします。
3. **ボリューム名**を入力します。
4. ボリュームのサイズをギガバイト (GB) 単位で入力します。
5. **配置** で割り当て先となるクラウドテナントを選択します。
6. **追加** をクリックします。

重要

ボリュームの作成後は、ボリューム名のみが編集可能となります。

7.1.2. ボリュームのバックアップ作成

データ損失に備えてボリュームのバックアップを作成しておくと、問題が発生した場合でも復元することができます。

重要

ボリュームのバックアップ作成には、OpenStack Block Storage で **`openstack-cinder-backup`** サービスを有効にしている必要があります。

以下の方法でボリュームのバックアップを作成します。

1. **ストレージ** → **ボリューム** に移動します。
2. バックアップを作成するボリュームをクリックして、概要を開きます。
3. (**構成**) をクリックして、 (**このクラウドボリュームのバックアップの作成**) をクリックします。
4. **バックアップ名** に名前を入力します。
5. オプションで **インクリメンタルであるかどうか** を選択すると、完全バックアップではなく、増分バックアップが作成されます。

   注記

   ボリュームの完全バックアップが少なくとも 1 つある場合には、増分バックアップを作成できます。増分バックアップでは、そのボリュームが最後にバックアップされた時点以降に加えられた変更のみを取得するので、リソースが節約されます。詳細は、**『Red Hat OpenStack Platform ストレージガイド』** の 「ボリュームの増分バックアップの作成」 を参照してください。

6. **保存** をクリックします。

ボリュームの概要ページで **クラウドボリュームバックアップ** をクリックすると、バックアップが表示されます。

注記

バックアップについての詳細は、**『Red Hat OpenStack Platform ストレージガイド』** の 「ボリュームのバックアップと復元」 を参照してください。

7.1.3. バックアップからのボリュームの復元

データ損失時には、以下の方法でバックアップからボリュームを復元できます。

1. **ストレージ** → **ボリューム** に移動します。
2. 復元するボリュームのバックアップをクリックします。ボリュームの概要ページが開きます。
3. (**構成**) をクリックして、 (**このクラウドボリュームのバックアップからの復元**) をクリックします。
4. **クラウドボリュームバックアップ** 一覧から復元するボリュームを選択します。

5. **保存** をクリックします。

7.1.4. ボリュームのスナップショット作成

ボリュームのスナップショットを作成することで、ある時点のボリュームの状態を保持することができます。そのスナップショットを使用して、ボリュームの複製を作成することができます。

以下の方法でボリュームのスナップショットを作成します。

1. **ストレージ → ボリューム** に移動します。
2. スナップショットを作成するボリュームをクリックして、概要を開きます。
3. (**構成**) をクリックして、 (**このクラウドボリュームのスナップショットの作成**) をクリックします。
4. **スナップショット名** に名前を入力します。
5. **保存** をクリックします。

ボリュームの概要ページで **クラウドボリュームスナップショット** をクリックすると、スナップショットが表示されます。

注記

スナップショットについての詳細は、**『Red Hat OpenStack Platform ストレージガイド』** の「ボリュームスナップショットの作成、使用、削除」 を参照してください。

7.1.5. インスタンスへのボリュームの割り当て

以下の方法でボリュームを OpenStack インスタンスに割り当てます。

1. **ストレージ → ボリューム** に移動します。
2. 割り当てるボリュームを選択します。
3. (**構成**) をクリックして、 (**このクラウドボリュームのインスタンスへの割り当て**) をクリックすると **クラウドボリュームの割り当て** 画面が開きます。
4. 一覧からインスタンスを選択します。
5. オプションで、**デバイスマウントポイント** を入力します。
6. **割り当て** をクリックします。

7.1.6. インスタンスからのボリュームの割り当て解除

以下の方法でボリュームを OpenStack インスタンスから割り当て解除します。

1. **ストレージ → ボリューム** に移動します。
2. 割り当て解除するボリュームを選択します。

3. **(構成)** をクリックして、 **(インスタンスからのこのクラウドボリュームの割り当て解除)** をクリックすると **クラウドボリュームの割り当て解除** 画面が開きます。
4. 一覧からインスタンスを選択します。
5. **割り当て解除** をクリックします。

7.1.7. ボリュームの編集

既存ボリュームでは、ボリューム名のみが編集可能です。

以下の方法でボリューム名を編集します。

1. **ストレージ** → **ボリューム** に移動します。
2. 編集するボリュームを選択して概要ページを開きます。
3. **(構成)** をクリックして、 **(このクラウドボリュームの編集)** をクリックします。
4. 新しい **ボリューム名** を入力します。
5. **保存** をクリックします。

7.1.8. ボリュームの削除

以下の方法で OpenStack Block Storage マネージャーからボリュームを削除します。

1. **ストレージ** → **ボリューム** に移動します。
2. 削除するボリュームを選択します。
3. **(構成)** から **(このクラウドボリュームの削除)** をクリックします。

7.2. OPENSTACK OBJECT STORAGE MANAGERS

OpenStack Object Storage (**`openstack-swift`**) サービスは、クラウドオブジェクトストレージを提供します。

OpenStack Object Storage をストレージマネージャーとして使用するには、まず OpenStack クラウドプロバイダーを Red Hat CloudForms アプライアンスに追加して、イベントを有効にする必要があります。 CloudForms が自動的に Object Storage サービスを発見し、Red Hat CloudForms 内の **Storage Managers** リストに追加します。クラウドプロバイダーの追加とイベントの有効化については、「OpenStack プロバイダーの追加」 を参照してください。

7.2.1. オブジェクトストアの表示

オブジェクトストアの概要ページでは、オブジェクトストアのサイズ、parent クラウド、ストレージマネージャー、クラウドテナント、およびオブジェクトストア上のクラウドオブジェクト数などの詳細が表示されます。

Red Hat CloudForms では、以下の方法でオブジェクトストレージマネージャー上のオブジェクトストアを表示できます。

1. **ストレージ** → **オブジェクトストア** に移動してオブジェクトストアコンテナーの一覧を表示します。
2. コンテナーをクリックして、概要ページを開きます。
3. **クラウドオブジェクト** をクリックして、オブジェクトストアコンテナー内のオブジェクトストアを一覧表示します。
4. 一覧からオブジェクトストアをクリックすると、概要ページが表示されます。