



Red Hat CloudForms 4.6

プロバイダーの管理

インフラストラクチャー、クラウド、コンテナプロバイダーの管理

Red Hat CloudForms 4.6 プロバイダーの管理

インフラストラクチャー、クラウド、コンテナプロバイダーの管理

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

法律上の通知

Copyright © 2018 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

概要

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、コンテナプロバイダーの管理およびシステムマネージャー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くと、より迅速に対応することができます。

目次

前書き	5
第1章 インフラストラクチャープロバイダー	6
1.1. インフラストラクチャープロバイダーの検出	6
1.2. 物理インフラストラクチャープロバイダーの検出	7
1.3. RED HAT VIRTUALIZATION プロバイダー	7
1.3.1. Red Hat Virtualization 容量および使用状況のデータ収集の有効化	7
1.3.2. Red Hat Virtualization プロバイダーの追加	8
1.3.3. Red Hat Virtualization ホストの認証	9
1.4. OPENSTACK インフラストラクチャープロバイダー	10
1.4.1. OpenStack インフラストラクチャープロバイダーの追加	10
1.4.1.1. アンダークラウドでイベントを保管するための設定	12
1.5. VMWARE VCENTER プロバイダー	12
1.5.1. VMware vCenter プロバイダーの追加	13
1.5.1.1. vCenter ホストに管理者以外のアカウントを使用する方法	13
1.5.2. VMware vCenter ホストの認証	14
1.6. MICROSOFT SCVMM プロバイダー	15
1.6.1. Microsoft SCVMM に対する認証	15
1.6.2. Microsoft SCVMM プロバイダーの追加	16
1.7. プロバイダーの更新	17
1.8. 複数のプロバイダーのタグ付け	17
1.9. プロバイダーの表示	17
1.10. プロバイダーの削除	19
1.11. プロバイダーのタイムラインの表示	19
1.12. ホストとクラスターの表示	20
1.13. 仮想マシンとテンプレートの表示	21
第2章 設定管理プロバイダー	22
2.1. RED HAT SATELLITE 6	22
2.1.1. ワークフローの定義	22
2.1.2. ホストグループ階層の定義	22
2.1.3. Satellite 6 プロバイダーの追加	22
2.1.4. Satellite 6 プロバイダーの更新のトリガー	23
2.1.5. Red Hat Satellite 6 のコンテンツの表示	23
2.1.6. ベアメタルホストの再プロビジョニング	24
2.1.7. ベアメタルホストのタグ付け	25
第3章 自動化管理プロバイダー	26
3.1. ANSIBLE	26
3.1.1. Embedded Ansible サーバーロールの有効化	26
3.1.2. Embedded Ansible ワーカーの状態の確認	27
3.1.3. Playbook のリポジトリの追加	27
3.1.4. リポジトリの更新	27
3.1.5. 認証情報の追加	28
3.1.6. 認証情報	28
3.1.6.1. 認証情報の追加	28
3.1.6.2. 認証情報タイプ	29
3.1.6.2.1. マシン	29
3.1.6.2.2. ネットワーク	29
3.1.6.2.3. SCM	30
3.1.6.2.4. Amazon	30
3.1.6.2.5. Azure Classic (非推奨)	30

3.1.6.2.6. Azure	31
3.1.6.2.7. Google Compute Engine	31
3.1.6.2.8. OpenStack	31
3.1.6.2.9. Rackspace	31
3.1.6.2.10. Satellite 6	32
3.1.6.2.11. VMware	32
3.1.7. Red Hat CloudForms 向けの Ansible Playbooks の最適化	32
3.1.7.1. Embedded Ansible アプライアンスでのロールのインストール	32
3.1.7.2. Ansible サービスのリンク	33
3.1.7.2.1. 例: 仮想マシンのサービスへのリンク	33
3.1.7.3. manageiq-automate ロールを使用した自動化ワークスペースの変更	34
3.1.7.3.1. ロールの変数	34
3.1.7.3.2. Playbook の例	35
3.2. ANSIBLE TOWER	35
3.2.1. Ansible Tower プロバイダーの追加	36
3.2.2. Ansible Tower プロバイダーの更新	37
3.2.3. Ansible Tower プロバイダーとインベントリーの表示	38
3.2.4. Ansible Tower 構成済みシステム	38
3.2.5. サービスカタログからの Ansible Tower ジョブテンプレートの実行	39
3.2.6. カスタムの自動化ボタンを使用した Ansible Tower Job の実行	41
第4章 クラウドプロバイダー	45
4.1. OPENSTACK プロバイダー	45
4.1.1. OpenStack プロバイダーの追加	45
4.1.1.1. オーバークラウドでイベントを保管するための設定	49
4.2. AZURE プロバイダー	49
4.2.1. Azure プロバイダーの追加	49
4.2.2. Azure プロバイダーの検出	51
4.2.3. Azure クラウドリージョンの無効化	51
4.3. AMAZON EC2 プロバイダー	52
4.3.1. Amazon EC2 プロバイダーの権限	52
4.3.2. Amazon EC2 プロバイダーの追加	52
4.3.3. Amazon EC2 クラウドプロバイダーの検出	53
4.3.4. Amazon EC2 からのパブリック AMI の有効化	53
4.3.5. AWS Config の通知の有効化	54
4.3.6. Amazon クラウドリージョンの無効化	54
4.4. GOOGLE COMPUTE ENGINE プロバイダー	55
4.4.1. Google Compute Engine プロバイダーの追加	55
4.4.2. Google Compute Engine イベントの有効化	56
4.4.2.1. Google Compute Engine でイベントをエクスポートするための設定	57
4.4.2.2. Red Hat CloudForms での Google Compute Engine イベントの表示	58
4.5. クラウドプロバイダーの更新	59
4.6. クラウドプロバイダーのタグ付け	59
4.7. クラウドプロバイダーの削除	59
4.8. クラウドプロバイダーの編集	60
4.9. クラウドプロバイダーのタイムラインの表示	60
第5章 ネットワークマネージャー	62
5.1. ネットワークプロバイダーの追加/表示	62
5.2. ネットワークプロバイダーの更新	62
5.3. ネットワークプロバイダーのタグ付け	63
5.4. ネットワークプロバイダーの削除	63
5.5. ネットワークプロバイダーのタイムラインの表示	63

5.6. 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	64
第6章 ミドルウェア管理プロバイダー	66
6.1. ミドルウェアプロバイダーの追加	66
第7章 コンテナプロバイダー	68
7.1. OPENSIFT CONTAINER PLATFORM MANAGEMENT トークンの取得	69
7.1.1. OpenShift Container Platform 3.3 以降での管理トークンの取得	69
7.1.2. OpenShift Enterprise 3.2 の管理トークンの取得	69
7.1.3. OpenShift Enterprise 3.1 の管理トークンの取得	69
7.2. OPENSIFT CLUSTER メトリックの有効化	70
7.3. OPENSIFT CONTAINER PLATFORM プロバイダーの追加	70
7.4. コンテナプロバイダーのタグ付け	73
7.5. コンテナプロバイダーの削除	74
7.6. コンテナプロバイダーの一時停止/再開	74
7.7. コンテナプロバイダーの編集	74
7.8. コンテナプロバイダーの環境変数の非表示	77
7.9. コンテナプロバイダーのタイムラインの表示	78
7.10. コンテナの概要のページ	79
7.10.1. プロバイダー間共通のインサイト	79
7.10.2. コンテナの概要のページを使用した作業	79
7.10.2.1. オブジェクトの概要の表示	80
7.10.3. トポロジーウィジェットの使用	83
7.10.3.1. コンテナプロバイダーのトポロジーの表示	84
7.10.3.2. コンテナプロバイダープロジェクトのトポロジーの表示	84
7.10.3.3. トポロジービューに表示するコンテナ数の制限	84
7.10.4. SmartState 分析の実行	84
第8章 ストレージマネージャー	86
8.1. AMAZON ELASTIC BLOCK STORE マネージャー	86
8.2. OPENSTACK BLOCK STORAGE マネージャー	86
8.3. OPENSTACK OBJECT STORAGE MANAGERS	86
8.3.1. オブジェクトストアの表示	87
付録A 付録	88
A.1. 自己署名の CA 証明書の使用	88

前書き

Red Hat CloudForms は、プロバイダーやマネージャーとして知られるさまざまな外部な環境を管理できます。プロバイダーまたはマネージャーは、データの収集や操作の実行を目的に CloudForms が統合するシステムのことです。

CloudForms における **プロバイダー** は外部の仮想化、クラウド、またはコンテナ環境のことで、複数の仮想マシンや、複数のホスト上にあるインスタンスを管理します。たとえば、複数のホストや仮想マシンを管理するプラットフォームである Red Hat Virtualization などが一例です。

CloudForms における **マネージャー** とは複数の種類のリソースを管理する外部管理環境のことで、マネージャーの例として、インフラストラクチャー、クラウド、ネットワーク、ストレージリソースを管理する OpenStack が挙げられます。

本書は、以下のような CloudForms におけるプロバイダーとマネージャーとの連携について説明します。

- インフラストラクチャープロバイダー
- 設定管理プロバイダー
- 自動化管理プロバイダー
- クラウドプロバイダー
- ネットワーク管理プロバイダー
- ミドルウェア管理プロバイダー
- コンテナプロバイダー
- ストレージマネージャー

プロバイダーまたはマネージャーに含まれるリソースとの連携に関する情報は『[インフラストラクチャーおよびインベントリーの管理](#)』を参照してください。

第1章 インフラストラクチャプロバイダー

Red Hat CloudForms において、インフラストラクチャプロバイダーとは、CloudForms アプリケーション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環境のことを指します。本章では、CloudForms に追加可能なインフラストラクチャ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。インフラストラクチャプロバイダーは、CloudForms により自動的に検出させるか、個別で追加することができます。

Web インターフェースは、仮想サムネイルでインフラストラクチャ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



表1.1 プロバイダー認証ステータス

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 → 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. 物理インフラストラクチャプロバイダーの検出

CloudForms には、仮想インフラストラクチャプロバイダーの検出以外に、特定のサブネット範囲で物理インフラストラクチャプロバイダーを検出する機能が追加されました。

1. **コンピュー**ト → **物理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、 (**物理インフラストラクチャプロバイダーの検出**) を選択します。
3. **検出タイプ** でプロバイダーを選択します。
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。
5. **ポート** を入力します。
6. **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物理インフラストラクチャ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、認証情報を入力する必要があります。

1.3. RED HAT VIRTUALIZATION プロバイダー

Red Hat Virtualization 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。また、使用率の追跡や共通の問題の特定のため、容量および使用状況データを設定することもできます。

1.3.1. Red Hat Virtualization 容量および使用状況のデータ収集の有効化



以下を設定して、Red Hat Virtualization プロバイダーから容量および使用状況データを収集します。

- CloudForms で、**構成** → **サーバー** → **サーバー制御** の設定メニューから容量および使用状況のサーバーロールを有効化します。容量および使用状況の収集に関する情報は『**Deployment Planning Guide**』の「[Assigning the Capacity and Utilization Server Roles](#)」を参照します。
- データの収集に使用するクラスターとデータストアの選択に関する情報は、『**全般設定ガイド**』の「[容量と使用状況の収集](#)」を参照してください。
- Red Hat Virtualization 環境で、Data Warehouse および Reports のコンポーネントをインストールして、Data Warehouse データベースで Red Hat CloudForms ユーザーを作成します。
 - 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、『**データウェアハウスガイド**』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](#)」のセクションを参照してください。

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

Red Hat CloudForms 環境の初回インストール、作成の完了後に、Red Hat Virtualization Manager プロバイダーをアプライアンスに追加します。

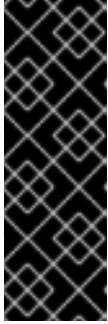
1. コンピュート → インフラストラクチャー → プロバイダー に移動します。
2.  (構成) をクリックして  (新規インフラストラクチャープロバイダーの追加) を選択します。
3. プロバイダーの **名前** を入力します。
4. **タイプ** の一覧から **Red Hat Virtualization** を選択します。
5. プロバイダー用に適切な **ゾーン** を選択します。ゾーンを指定しない場合は **default** に設定されます。
6. デフォルト タブの **エンドポイント** で以下を設定します。
 - プロバイダーの **ホスト名** か、IPv4 または IPv6 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指定する必要があります。

- 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。
 - **TLS 証明書の確認** で **はい** または **いいえ** を選択して、TLS を使用してプロバイダーへのセキュアな認証を行うかどうかを指定します。
 - **TLS 証明書の確認** で **はい** を選択した場合は、**信頼された CA 証明書** フィールドにカスタムの証明書を PEM 形式で貼り付けるか、Red Hat Virtualization に信頼済みの認証局がある場合には **信頼された CA 証明書** フィールドを空のままにします。
 - Red Hat Virtualization の管理者ユーザーのログイン認証情報を指定します。
 - **ユーザー名** フィールドに、**admin@internal** という形式の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 CloudForms が Red Hat Virtualization Manager に接続できることを確認します。
7. **C & U データベース** タブの **エンドポイント** で、Red Hat Virtualization Data Warehouse データベースの CloudForms ユーザーのログイン情報を入力して、容量および使用状況のメトリックの収集を設定できます。これは、後からプロバイダーを編集して設定することも可能です。**C & U データベース** タブで以下を設定します。





重要

Red Hat Virtualization プロバイダーから容量および使用状況データを収集するには、CloudForms で capacity and utilization server role を有効化する必要があります。Red Hat Virtualization 環境には、Data Warehouse および Reports コンポーネントと CloudForms ユーザーが含まれている必要があります。特定のクラスター、ホスト、データストアもデータ収集用に設定することができます。設定の詳細は「[Red Hat Virtualization 容量および使用状況のデータ収集の有効化](#)」を参照してください。

- **ホスト名** でデータベースのホスト名か、IPv4 または IPv6 アドレスを入力します。
 - 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。
 - **データベース名** を入力します。
 - **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、CloudForms がデータベースに接続できることを確認します。
8. **追加** をクリックして、Red Hat Virtualization プロバイダーの追加を完了します。

1.3.3. Red Hat Virtualization ホストの認証

Red Hat Virtualization インフラストラクチャーを追加した後は、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. **コンピューター → 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 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。

1.4. OPENSTACK インフラストラクチャプロバイダー



OpenStack インフラストラクチャ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。

1.4.1. OpenStack インフラストラクチャ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 Queuing 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 『[アーキテクチャガイド](#)』の [「OpenStack Telemetry \(ceilometer\)」](#)を参照してください。
- 自己署名の認証局 (CA) を使用してプロバイダーを認証するには、プロバイダーを追加する前に [「自己署名の CA 証明書の使用」](#) の手順に従い、CloudForms アプライアンスが証明書を信頼するように設定します。

1. コンピュート → インフラストラクチャ → 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。
- 作成中のプロバイダーには、指定のドメインのプロジェクトのみが表示されます。他のドメインのプロジェクトを表示するには別のクラウドプロバイダーとしてプロジェクトを追加してください。OpenStack のドメイン管理に関する情報は、『Red Hat OpenStack Platform **Users and Identity Management Guide**』の「[Domain Management](#)」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. **セキュリティープロトコル** の方法を選択して、プロバイダーの認証方法を指定します。
 - **検証なしの SSL**: SSL を使用してセキュアでない方法でプロバイダーを認証します。
 - **SSL**: 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。これは、推奨の認証方法です。
 - **非 SSL**: SSL なしの HTTP プロトコルのみでセキュアでない方法でプロバイダーに接続します。
 - b. 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)。
 - c. **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。
 - d. 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。

- e. **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。
 - 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。
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プロバイダーを設定した後は、**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 にアクセスする必要があります。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。

1.4.1.1. 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。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。

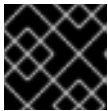
1.5. VMWARE VCENTER プロバイダー

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。

1.5.1. 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。

1.5.1.1. vCenter ホスト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。ロール作成の方法については、「[VMware ドキュメント](#)」を参照してください。

管理者以外のユーザーに対して、以下の特権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をチェックする必要があります。

- 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が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が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が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がある各 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。

1.5.2. 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. **コンピューター → 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。

1.6. MICROSOFT SCVMM プロバイダー

Microsoft System Center Virtual Machine Manager (SCVMM) 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 つが必要です。SCVMM ホストのプロパティで、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。

1.6.1. 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があります。

1. Microsoft SCVMM サーバーにログインします。
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"}
```

- 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"}'
```

- 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。



1.6.2. Microsoft SCVMM プロバイダーの追加

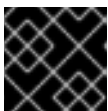
初回のインストールが完了し、Red Hat CloudForms 環境が作成された後に、Microsoft System Center Virtual Machine Manager (SCVMM) プロバイダーをアプライアンスに追加します。



注記

自己署名の認証局 (CA) を使用してプロバイダーを認証するには、プロバイダーを追加する前に「[自己署名の CA 証明書の使用](#)」の手順に従い、CloudForms アプライアンスが証明書を信頼するように設定します。

- コンピューター → インフラストラクチャー → プロバイダー に移動します。
-  (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。
- 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。
- タイプ** の一覧から **Microsoft System Center VMM** を選択します。
- 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。


- セキュリティプロトコル の一覧から **Kerberos** または **基本 (SSL)** を選択します。
 - Kerberos** の場合:
 - 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。
 - 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** 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。

1.7. 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 → 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。

1.8. 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 → 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。



Select a customer tag to assign: Environment *		
		<Select a value to assign>
	Category	Assigned Value
	Cost Center *	Cost Center 001
	Environment *	Quality Assurance

* Only a single value can be assigned from these categories

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。

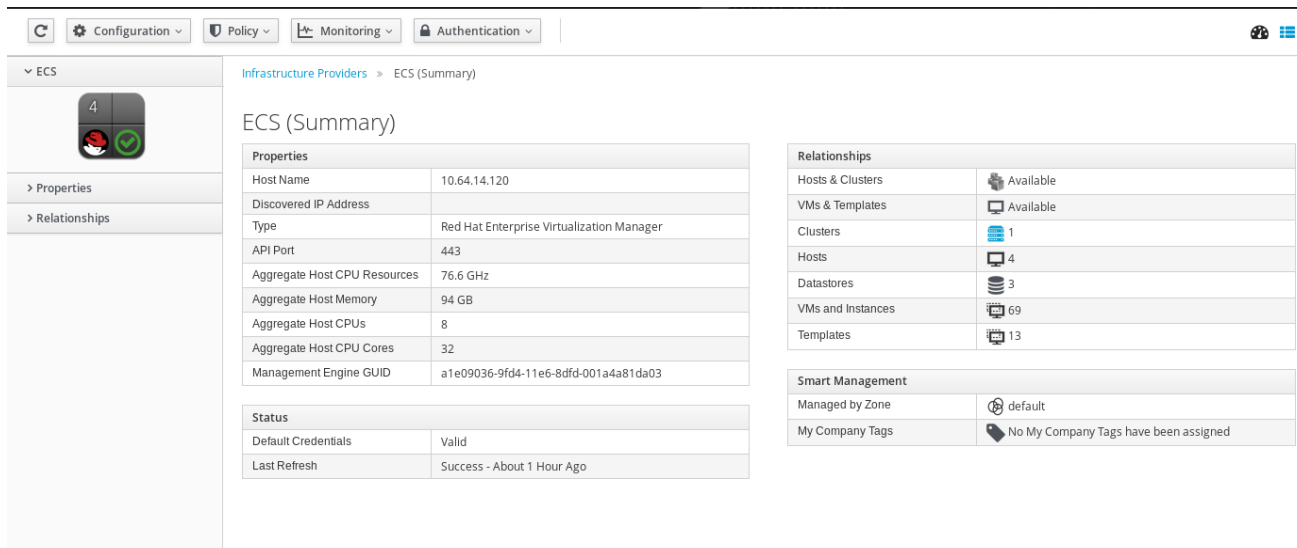
1.9. プロバイダーの表示

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












Infrastructure Providers > ECS (Summary)

ECS (Summary)

Properties	
Host Name	10.64.14.120
Discovered IP Address	
Type	Red Hat Enterprise Virtualization Manager
API Port	443
Aggregate Host CPU Resources	76.6 GHz
Aggregate Host Memory	94 GB
Aggregate Host CPUs	8
Aggregate Host CPU Cores	32
Management Engine GUID	a1e09036-9fd4-11e6-8dfd-001a4a81da03

Status	
Default Credentials	Valid
Last Refresh	Success - About 1 Hour Ago

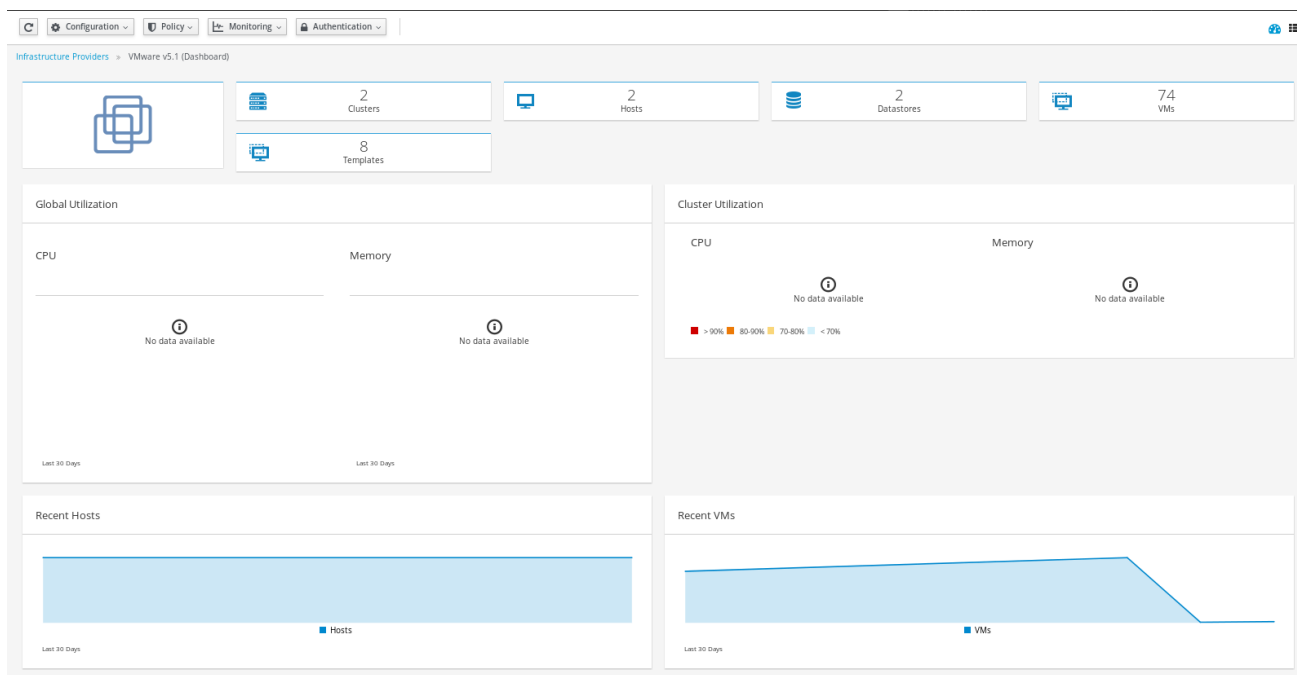
Relationships	
Hosts & Clusters	 Available
VMs & Templates	 Available
Clusters	 1
Hosts	 4
Datastores	 3
VMs and Instances	 69
Templates	 13

Smart Management	
Managed by Zone	 default
My Company Tags	 No My Company Tags have been assigned






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** 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**、**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



Infrastructure Providers > VMware v5.1 (Dashboard)

 2 Clusters
  2 Hosts
  2 Datastores
  74 VMs
  8 Templates

Global Utilization

CPU

Memory

No data available

No data available

Cluster Utilization

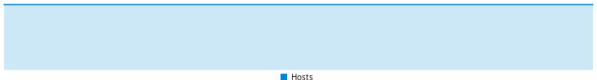
CPU

Memory

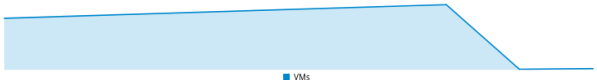
No data available

No data available

Recent Hosts




Recent VMs



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の数。エンティティをクリックすると、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。

1.10. 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。

1.11. 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 → 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。

Options

Show	Management Events	▼
------	-------------------	---

Interval	Daily	▼
Date	11/20/2015	
Show	7	▼ days back

Level	Summary	▼
Event Groups	Power Activity	▼
	<NONE>	▼
	<NONE>	▼

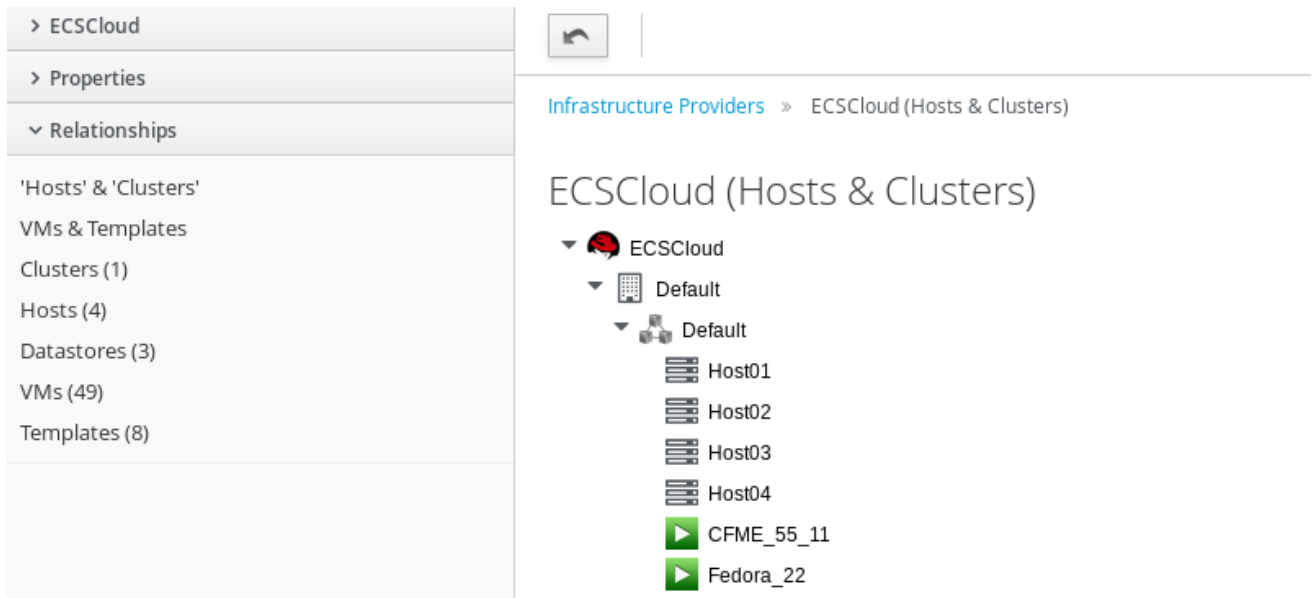
* Dates/Times on this page are based on time zone: UTC.

- **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。

1.12. 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。



1.13. 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

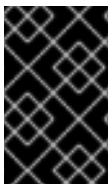
CloudForms における構成管理プロバイダーは、CloudForms アプライアンスに追加してリソースのライフサイクルを管理可能なシステム管理製品です。構成管理プロバイダーは、プロバイダー全体に同じ変更や更新を適用したり、状況や変更アクティビティを記録、レポートしたりする場合に便利です。またこのようなプロバイダーは、異なるプロバイダーが存在することでもたらされる混乱や間違いをなくするために役立つ場合もあります。

本章は、CloudForms で利用可能な異種の構成管理プロバイダーや、その管理方法について説明します。構成管理プロバイダーは個別に CloudForms に追加する必要があります。

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ニングするのみです。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 Satellite 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。

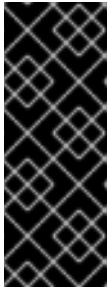
2.1.6. ベアメタルホストの再プロビジョニング

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
 - 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は 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。

第3章 自動化管理プロバイダー

Red Hat CloudForms における自動化管理プロバイダーは、CloudForms を統合してリソースの自動化操作を簡素化する管理ツールです。本章は、Red Hat CloudForms で利用可能な自動管理プロバイダーとその連携方法について説明します。

Red Hat CloudForms は、以下により自動化管理機能を提供します。

自動化 では、リアルタイムの双方向のプロセス統合が可能です。自動化では、管理イベントや管理または運用アクティビティー向けの適応型の自動化を実装する手段を提供します。

Ansible の統合により、カスタマイズすることなく、Ansible Playbook を使用してサービス、アラート、ポリシーアクションをバックアップするサポートが追加されました。既存の Playbook のリポジトリと CloudForms を同期して、プロバイダーにアクセスするための認証情報を追加し、仮想マシンの作成やリタイア、セキュリティソフトウェアの更新、容量が少なくなった場合のさらなるディスクの追加などのアクション向けのサービスカタログアイテムを作成します。

Ansible Tower は、CloudForms に統合された管理ツールで、お使いのインベントリで、既存の Ansible Tower プロバイダーを使用してインフラストラクチャーの運用を自動化するために設計されています。CloudForms では、サービスカタログや自動化を使用して Ansible Tower のジョブを実行できます。Ansible Tower を使用すると、Ansible Playbook の実行のスケジュールや、現在または過去の結果の監視が可能で、問題が発生する前に問題のトラブルシューティングや特定が可能になります。

3.1. ANSIBLE

Ansible が Red Hat CloudForms に統合され、Playbook を使用することでサービス、ポリシー、警告アクションの自動化ソリューションが提供されるようになりました。Ansible Playbook は、インベントリと呼ばれるホスト全体での自動化を定義する一連の **プレイ** またはタスクで構成されています。

単純なタスクから複雑なタスクまで、Ansible Playbook でクラウド管理をサポートできます。

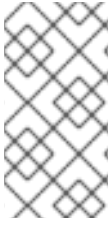
- **サービス**: Playbook で CloudForms のサービスカタログアイテムをバックアップできるようにします。
- **コントロールアクション**: CloudForms ポリシーは、プロバイダーからのイベントをベースにしたアクションとして Playbook を実行できます。
- **コントロールアラート**: CloudForms アラートの指示できるように Playbook を設定します。

Ansible は、インストールの必要がないように CloudForms に組み込まれています。Red Hat CloudForms で Ansible を使用する際の基本的なワークフローは以下のとおりです。

1. **Embedded Ansible** サーバーロールを有効化すること
2. Playbook が含まれるソースのコントロールリポジトリを追加すること
3. インベントリとの認証情報を確立すること
4. 利用可能な Playbook を使用して、サービス、アラート、ポリシーをバックアップすること

3.1.1. Embedded Ansible サーバーロールの有効化

Red Hat CloudForms では、**Embedded Ansible** ロールはデフォルトで無効になっています。Ansible Automation Inside を使用するには、このサーバーロールを有効化します。



注記

CloudForms アプライアンスネットワークのアイデンティティ (ホスト名/IP アドレス) を設定してから、Embedded Ansible サーバーロールを有効にします。ホスト名や IP アドレスに変更を加えてから、有効化した Embedded Ansible サーバーロールを使用して、アプライアンス上の **evmservd** サービスを再起動します。

1. 設定メニューから **構成** → **設定** を選択します。
2. **ゾーン** で任意のサーバーを選択します。
3. **Embedded Ansible** の **サーバーロール** を **On** に設定します。

3.1.2. Embedded Ansible ワーカーの状態の確認

Embedded Ansible ワーカーが起動してその機能を使用していることを確認します。

1. 設定メニューから **構成** → **診断** を選択して、任意のサーバーをクリックします。
2. **ワーカー** タブをクリックします。

全ワーカーおよび現在の状況の表が表示され、埋め込み Ansible ワーカーの状況を確認できます。

3.1.3. Playbook のリポジトリの追加

Red Hat CloudForms が Playbook を検出して公開できるようにリポジトリを追加します。

1. **自動化** → **Ansible** → **リポジトリ** の順に移動します。
2. **追加** をクリックします。
3. **名前** フィールドにリポジトリ名を指定します。
4. **説明** フィールドにリポジトリの説明を入力します。
5. ドロップダウンメニューから **SCM タイプ** を選択します。
6. リポジトリの **URL** または IP アドレスを追加します。
7. ドロップダウンメニューから適切な **認証情報 (SCM)** を選択します。
8. **SCM ブランチ** フィールドでブランチ名を指定します。
9. **SCM Update Options** の適切なボックスにチェックを入れます。
10. **追加** をクリックします。

リポジトリを同期すると、Playbook は CloudForms で利用できるようになります。



3.1.4. リポジトリの更新

Red Hat CloudForms は、対象となる Playbook のリポジトリまたは、インベントリー内の全リポジトリを更新して、Playbook を最新の状態に保つことができます。

対象のリポジトリを更新します。

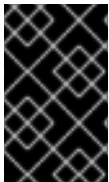
1. 自動化 → **Ansible** → **リポジトリ** の順に移動します。
2. リポジトリをクリックします。
3.  (構成) をクリックしてから、 (**Refresh this Repository**) をクリックします。

または、一覧からのリポジトリのすべてまたは一部を更新することができます。

1. 自動化 → **Ansible** → **リポジトリ** の順に移動します。
2. 更新するこれらのリポジトリを確認します。**すべてを選択** をクリックして全リポジトリを選択します。
3.  (構成)、 (**Refresh Selected Ansible Repositories**) の順に選択します。



3.1.5. 認証情報の追加

Red Hat CloudForms は、Playbook で使用する認証情報を保存できます。CloudForms に保存されている認証情報は、実行時に Playbook と照合され、実行されます。



重要

CloudForms と VMware プロバイダーが同じ IPv6 のみのネットワークに配置されている場合は、**vCenter Host** フィールドの VMware プロバイダーに DNS 解決可能なホスト名を使用して、認証情報の追加してください。

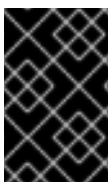
1. 自動化 → **Ansible** → **認証情報** の順に移動します。
2.  (設定) から  (**新規認証情報の追加**) をクリックします。
3. 認証情報に **名前** を指定します。
4. **Credential Type** を選択します。選択したタイプによっては、追加のフィールドが表示されます。
5. **追加** をクリックします。

3.1.6. 認証情報

Red Hat CloudForms は、マシンに対する Ansible Playbook の実行、インベントリソースとの同期、バージョン管理システムからのプロジェクトコンテンツのインポート時に認証情報を使用して認証します。



3.1.6.1. 認証情報の追加

Red Hat CloudForms は、Playbook で使用する認証情報を保存できます。CloudForms に保存されている認証情報は、実行時に Playbook と照合され、実行されます。



重要

CloudForms と VMware プロバイダーが同じ IPv6 のみのネットワークに配置されている場合は、**vCenter Host** フィールドの VMware プロバイダーに DNS 解決可能なホスト名を使用して、認証情報の追加してください。

1. 自動化 → **Ansible** → **認証情報** の順に移動します。
2.  (設定) から  (新規認証情報の追加) をクリックします。
3. 認証情報に **名前** を指定します。
4. **Credential Type** を選択します。選択したタイプによっては、追加のフィールドが表示されます。
5. **追加** をクリックします。

3.1.6.2. 認証情報タイプ

以下のセクションで、CloudForms が使用する各認証情報タイプを説明します。

3.1.6.2.1. マシン

マシンの認証情報により、CloudForms は管理対象のホストで Ansible を起動できます。コマンドラインで Ansible を使用するように、SSH ユーザー名や、オプションでパスワードや SSH キー、キーのパスワードを指定できます。これらの情報は ssh および Playbook のユーザーレベルの権限昇格のアクセスを定義し、リモートホストで Playbook を実行時に使用されます。

- **ユーザー名**: SSH 認証に使用されるユーザー名。
- **パスワード**: SSH 認証に使用される実際のパスワード。
- **SSH 秘密鍵**: マシンの認証情報についての SSH 秘密鍵をコピーするか、またはドラッグアンドドロップします。
- **秘密鍵のパスフレーズ**: 使用される SSH 秘密鍵がパスワードで保護される場合、秘密鍵のパスワードを設定できます。
- **権限昇格**: 特定のユーザーに割り当てる、昇格権限タイプを指定します。オプションには **sudo**、**su**、**pbrun**、**pfexec** が含まれます。
- **権限昇格のユーザー名**: リモートシステムで権限昇格で使用するユーザー名を入力します。
- **権限昇格のパスワード**: リモートシステムでの選択した権限昇格タイプでユーザーを認証するために使用される実際のパスワードを入力します。
- **Vault パスワード**: Ansible Vault の認証情報には、設定可能な **Vault パスワード** 属性のみが含まれます。



注記

Ansible Vault についての詳しい情報は、[「Using Vault in playbooks」](#) を参照してください。

3.1.6.2.2. ネットワーク

ネットワーク認証情報は、ネットワークデバイスへの接続およびその管理を実行するために Ansible ネットワークモジュールによって使用されます。

ネットワークの認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** ネットワークデバイスと併用するユーザー名。
- **パスワード:** ネットワークデバイスと併用するパスワード。
- **認証:** これを「オプション」フィールドから選択して、パスワードで RSA 鍵に署名する認証パスワードを追加します。
- **パスワードの認証:** 認証 にチェックが付いている場合は、**パスワードの認証** フィールドにパスワードを入力してください。
- **SSH 鍵:** ユーザーを SSH 経由でネットワークに対して認証するために使用される実際の SSH 秘密鍵をコピーするか、またはドラッグアンドドロップします。
- **秘密鍵のパスフレーズ:** ユーザーを SSH 経由でネットワークに対して認証するために使用する秘密鍵の実際のパスフレーズ。

3.1.6.2.3. SCM

SCM (ソースコントロール) 認証情報は、ローカルソースコードのリポジトリを、Git、Subversion、または Mercurial などのリモートのリビジョンコントロールシステムからクローン作成したり、更新したりするためにプロジェクトで使用されます。

ソースコントロールの認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** ソースコントロールシステムと併用するユーザー名。
- **パスワード:** ソースコントロールシステムと併用するパスワード。
- **秘密鍵のパスフレーズ:** 使用される SSH 秘密鍵がパスフレーズで保護される場合、その秘密鍵のパスフレーズを設定できます。
- **秘密鍵:** ユーザーを SSH 経由でソースコントロールシステムに対して認証するために使用される実際の SSH 秘密鍵をコピーするか、またはドラッグアンドドロップします。

3.1.6.2.4. Amazon

この認証情報タイプを選択すると、クラウドインベントリーの Amazon Web Services との同期が可能になります。

- **アクセスキー:** Amazon Web Service へのプログラム呼び出しを可能にするユーザーの認証情報
- **秘密鍵:** ユーザーのアクセスキーに対応する秘密鍵
- **STS トークン:** Amazon Web Services Security Token Service で生成されるトークン

3.1.6.2.5. Azure Classic (非推奨)

この認証情報タイプを選択すると、クラウドインベントリーと Microsoft Windows Azure Classic との同期が可能になります。

Microsoft Azure の認証情報には、設定可能ないくつかの属性があります。

- **サブスクリプション ID:** Microsoft Azure Classic アカountのサブスクリプション UUID。
- **管理証明書:** Microsoft Azure Classic コンソールでアップロードした証明書に対応する PEM ファイル。

3.1.6.2.6. Azure

この認証情報タイプを選択すると、クラウドインベントリーと Microsoft Azure との同期が可能になります。

Microsoft Azure の認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** Microsoft Azure アカウントへの接続に使用するユーザー名。
- **パスワード:** Microsoft Azure アカウントへの接続に使用するパスワード。
- **サブスクリプション ID:** Microsoft Azure アカウントのサブスクリプション UUID。
- **テナント ID:** Microsoft Azure アカウントのテナント ID。
- **クライアントシークレット:** Microsoft Azure アカウントのクライアントシークレット。
- **クライアント ID:** Microsoft Azure アカウントのクライアント ID。

3.1.6.2.7. Google Compute Engine

この認証情報タイプを選択すると、クラウドインベントリーと Google Compute Engine との同期が可能になります。

Google Compute Engine の認証情報には、設定可能ないくつかの属性があります。

- **サービスアカウントのメールアドレス:** Google Compute Engine サービスアカウントに割り当てられるメールアドレス。
- **RSA 秘密鍵:** サービスアカウントメールに関連付けられる PEM ファイル。
- **プロジェクト:** GCE によって割り当てられる識別情報です。これは、以下のように 2 語とそれに続く 3 桁の数字で構成されます (例: squeamish-ossifrage-123)。

3.1.6.2.8. OpenStack

この認証情報タイプを選択すると、クラウドインベントリーと Red Hat OpenStack との同期が可能になります。

OpenStack の認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** OpenStack への接続に使用するユーザー名。
- **パスワード (API キー):** OpenStack に接続するために使用するパスワードまたは API キー
- **ホスト (認証 URL):** 認証に使用するホスト。
- **プロジェクト (テナント名):** OpenStack に使用されるテナント名またはテナント ID。通常、この値はユーザー名と同じです。
- **ドメイン名:** OpenStack への接続に使用する FQDN。

3.1.6.2.9. Rackspace

この認証情報タイプを選択すると、クラウドインベントリーと Rackspace との同期が可能になります。

Rackspace の認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** vCenter への接続に使用するユーザー名。
- **API キー:** 管理者 ID に関連する公開鍵

3.1.6.2.10. Satellite 6

この認証情報タイプを選択すると、クラウドインベントリーと Red Hat Satellite 6 との同期が可能になります。

Satellite の認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** Satellite 6 への接続に使用するユーザー名。
- **パスワード:** Satellite 6 への接続に使用するパスワード。
- **Satellite 6 ホスト:** 接続先の Satellite 6 URL または IP アドレス。

3.1.6.2.11. VMware

この認証情報タイプを選択すると、インベントリーと VMware vCenter との同期が可能になります。



重要

CloudForms と VMware プロバイダーが同じ IPv6 のみのネットワークに配置されている場合は、**vCenter Host** フィールドの VMware プロバイダーに DNS 解決可能なホスト名を使用して、認証情報の追加してください。

VMware の認証情報には、設定可能ないくつかの属性があります。

- **ユーザー名:** vCenter への接続に使用するユーザー名。
- **パスワード:** vCenter への接続に使用するパスワード。
- **vCenter ホスト:** 接続先の vCenter ホスト名または IP アドレス。



注記

VMware ゲストツールがインスタンスで実行されていない場合、VMware インベントリーの同期により、そのインスタンスの IP アドレスが返されない場合があります。

3.1.7. Red Hat CloudForms 向けの Ansible Playbooks の最適化

Ansible は、単純なモデル駆動型の設定管理、マルチノードデプロイメント、リモートタスク実行に対応するシステムです。CloudForms で使用するために Playbook を設計すると、Playbook 自体でソリューションを活用して、Playbook でサポートされるサービスや自動化プロセスを最適に実装するのに便利です。

このセクションでは、Ansible Playbook に関する既存のドキュメントを補完するもので、管理者に対して CloudForms で使用するために Playbook を最適化する方法について説明します。

3.1.7.1. Embedded Ansible アプライアンスでのロールのインストール

ロールとは、既知のファイル構造をもとに、特定の変数ファイル、タスク、ハンドラーを自動的に読み

込む手段のことです。ロール別にコンテンツをグループ化すると、他のユーザーとロールを簡単に共有することができます。Playbook を最適化するためにアクティブ化された Embedded Ansible サーバーロールで、Red Hat CloudForms アプライアンスにロールをインストールします。

CloudForms アプライアンス上の Playbook でこのロールを使用する場合には、Playbook の root に空の **roles** ディレクトリーを追加します。この **roles** ディレクトリーに、以下の内容を含む **requirements.yml** ファイルを追加してください。

```
---
- src: <ansible-galaxy-role>
```

CloudForms は、Playbook 内で **requirements.yml** ファイルを検出すると、このロールを自動的にインストールします。

3.1.7.2. Ansible サービスのリンク

Red Hat CloudForms は、Ansible Playbook を使用して作成した仮想マシンなどのインベントリーリソースが、リソースの生成に使用したサービスにリンクできるように、モジュールを提供します。Playbook のサービスオーダー中に、**add_provider_vms** モジュールにより、Playbook がワーカーアプライアンスに接続し直されて、生成を行ったプロバイダーリソースを特定します。リンクが済むと、新たに生成されたリソースは CloudForms のライフサイクル管理機能で利用できるようになります。

作成したサービスに、仮想マシンをリンクし直すには、プロビジョニングに使用した Playbook で以下のタスクを実装する必要があります。

1. リソースを作成して、そのリソースを登録する
2. **add_provider_vms** メソッドを使用してサービスを新規作成したリソースにリンクする

3.1.7.2.1. 例: 仮想マシンのサービスへのリンク

以下の Playbook のタスクの例では、仮想マシンが Amazon EC2 にデプロイされて、サービスにリンクし直されます。リソースとサービスを **href slug** や、オブジェクトとしてリンクする例を紹介します。

注記

- この例では、``syncrou.manageiq-vmdb`` ロールを使用します。このロールを使用すると、CloudForms ユーザーが Ansible Playbook を使用して VMDB オブジェクトを変更、修正することができます。CloudForms 向けに Ansible Playbook を記述する場合のロールの実装や使用に関する詳しい情報は、[「Embedded Ansible アプライアンスでのロールのインストール」](#)を参照してください。
- Ansible Galaxy およびロールに関する詳細情報は、[「Ansible Galaxy documentation」](#)を参照してください。
- サービスを正しくリンクできるように、プロバイダー ID をメモしてください。

1. リソースを作成して、登録します。

```
- name: Create Ec2 Instance
  ec2:
    key_name: "{{ key }}"
    instance_tags: {Name: "{{ name }}" }
    group_id: "{{ security_group }}"
    instance_type: "{{ instance_type }}"
```

```

region: "{{ region }}"
image: "{{ image }}"
wait: yes
count: 1
vpc_subnet_id: "{{ subnet }}"
assign_public_ip: yes
register: ec2

```

2. **add_provider_vms** メソッドを、**href slug** またはオブジェクト経由でサービスにリンクするアクションとして呼び出します。

```

- name: Service Linking via an href slug
  manageiq_vmdb:
    href: "href_slug::services/80"
    action: add_provider_vms
    data:
      uid_ems:
        - "{{ ec2.instances[0].id }}"
      provider:
        id: 24

- name: Service Linking via an object
  manageiq_vmdb:
    vmdb: "{{ vmdb_object }}"
    action: add_provider_vms
    data:
      uid_ems:
        - "{{ ec2.instances[0].id }}"
      provider:
        id: 24

```

3.1.7.3. manageiq-automate ロールを使用した自動化ワークスペースの変更

manageiq-automate ロールは、Red Hat CloudForms の自動化を使用するユーザーが Ansible Playbook を使用して自動化ワークスペースに変更、追加を加えることができます。

注記

Embedded Ansible がアクティブ化された Red Hat CloudForms アプライアンス上の Playbook でこのロールを使用する場合には、Playbook の root に空の **roles** ディレクトリーを追加します。この **roles** ディレクトリーに、以下の内容を含む **requirements.yml** ファイルを追加してください。

```

---
- src: syncrou.manageiq-automate

```

CloudForms は、Playbook 内で **requirements.yml** ファイルを検出すると、このロールを自動的にインストールします。

3.1.7.3.1. ロールの変数

manageiq_automate ロールは、CloudForms アプライアンスでの Playbook 実行を実装する時に、以下の変数を採用します。変数は **defaults/main.yml** と **vars/main.yml** に定義されます。

auto_commit: デフォルトでは **True** に設定されています。False に設定すると、**manageiq_automate** モジュールの **set_** メソッドへの CloudForms の各呼び出しに自動的にコミットされなくなります。

manageiq_validate_certs: デフォルトでは **True** に設定されています。**extra_vars** で渡される場合や Playbook の変数に割り当てられる場合には、SSL REST API 接続の URL の使用時に自己署名の証明書を検索に使用することができます。

3.1.7.3.2. Playbook の例

以下の例では **manageiq-automate** ロールを使用します。変数置換を使用する場合は、Playbook のタスクはメソッドパラメーターを取得して、オブジェクト属性を変更するために使用されます。最終的なタスクでは、**set_retry** モジュールを使用して、再試行の間隔を更新します。

```
- name: Siphon Method Parameters into an object
  hosts: localhost
  connection: local
  vars:
    - auto_commit: True
    - object: root
    - interval: 600

gather_facts: False
roles:
  - syncrou.manageiq-automate

tasks:
  - name: "Get the list of Method Parameters"
    manageiq_automate:
      workspace: "{{ workspace }}"
      get_method_parameters: yes
      register: method_params

  - name: "Set attributes"
    manageiq_automate:
      workspace: "{{ workspace }}"
      set_attributes:
        object: "{{ object }}"
        attributes: "{{ method_params.value }}"

  - name: Set Retry
    manageiq_automate:
      workspace: "{{ workspace }}"
      set_retry:
        interval: "{{ interval }}"
```

3.2. 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、Playbook 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 Playbook 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

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 Playbook 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、問題が発生する前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 Playbook を作成します。
2. 新しい Ansible Tower ジョブテンプレートは、Playbook から作成され、Red Hat CloudForms によって取得されます。
3. Ansible Tower ジョブテンプレートから、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 Playbook についての詳しい情報は、[Ansible Playbook のドキュメント](#) を参照してください。

3.2.1. 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. **自動化** → **Ansible Tower** → **エクスプローラー** の順に移動し、**プロバイダー** アコーディオンタブをクリックします。
2.  **構成** で  **新規プロバイダーの追加** をクリックします。
3. **新規プロバイダーの追加** エリアで以下を行います。

Providers

- All Configuration Management Providers
 - Red Hat Satellite Providers
 - Ansible Tower Providers
- Configured Systems
- Ansible Tower Job Templates

Add a new Configuration Management Provider

Name Required

Type

- <Choose>
- Ansible Tower
- Red Hat Satellite

Zone

Url Required

Verify Peer Certificate ☐

Credentials

Username Required

Password Required

Confirm Password Required

Required. Should have privileged access, such as root or administrator.

- 新規プロバイダーの **名前** を入力します。
 - プロバイダーの **ゾーン** を入力します。
 - 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。
- 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。
 - 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。
 - 検証** をクリックして認証情報を検証します。
 - 追加** をクリックします。

Ansible Tower プロバイダーを追加した後は、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。

3.2.2. 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、Playbook 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. **自動化** → **Ansible Tower** → **エクスプローラー** の順に移動し、**プロバイダー** アコーディオンタブをクリックします。
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ジョブテンプレートのインベントリーを取得します。

3.2.3. 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 ジョブ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ジョブ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. **自動化** → **Ansible Tower** → **エクスプローラー** の順に移動します。
2. **プロバイダー** アコーディオンメニューを選択して **すべての Ansible Tower 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、検出されたジョブテンプレートには、**自動化** → **Ansible Tower** → **エクスプローラー** → **ジョブテンプレート** アコーディオンメニューを展開し、プロバイダーの下からアクセスできます。

3.2.4. 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. **自動化** → **Ansible Tower** → **エクスプローラー** → **構成済みシステム** の順に移動します。

2. すべての **Ansible Tower 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。

3.2.5. サービスカタログからの **Ansible Tower** ジョブテンプレートの実行



Ansible Tower ジョブ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 Playbook を実行することができます。







重要

まず最初に、Ansible Tower でジョブ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atalog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. **自動化** → **Ansible Tower** → **ジョブ** の順に移動します。
2. **Ansible Tower ジョブテンプレート** 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、 (**このジョブ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。Playbook 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。

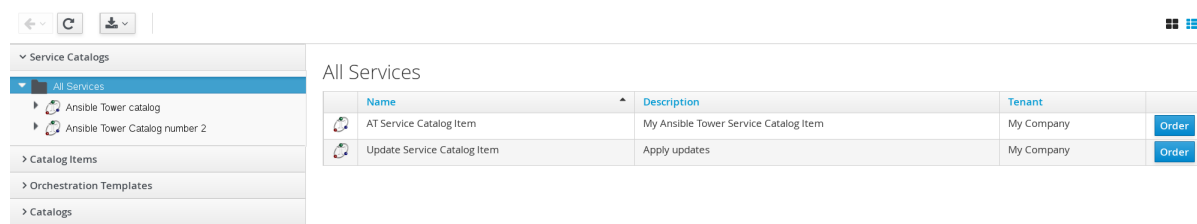
- **プロバイダー** でお使いの Ansible Tower プロバイダーを選択すると、**Ansible Tower ジョブテンプレート** オプションが表示され、**プロビジョニングのエントリーポイントのステートマシン** が自動的に設定されます。
- 該当する場合には **エントリーポイントの再設定** および **リタイアのエントリーポイント** の設定情報を追加します。
- 一覧から必要な **Ansible Tower ジョブテンプレート** を選択します。通常、これには、サービスダイアログの作成に使用した Ansible Tower Job テンプレートを選択します。

Adding a new Service Catalog Item

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atalog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。

3.2.6. 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 Playbook。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** → **自動化** → **カスタマイズ** の順に移動します。
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。Playbook 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 ジョブ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。

Adding a new Button


The screenshot shows the 'Adding a new Button' configuration page. It includes sections for defining the button's action, object details, attributes, and visibility. The 'Attribute/Value Pairs' section is a table with 5 rows for defining key-value pairs for the button.

Attribute/Value Pairs	1	2	3	4	5
job_template_name	first_job_template				

- **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** → **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。

Adding a new Buttons Group

Basic Info

Button Group Text: ☒ Display on Button

Button Group Hover Text:

Button Group Image:

Assign Buttons

Unassigned:

Selected:

- **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するには、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** → **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 ジョブ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。

Configuration Policy Monitoring Power Package Updates Update foo

VMs & Templates

All VMs & Templates

Dan's Director

> A <Archived>

> O <Orphaned>

> VMs

> Templates

VM and Instance "RHEL7-ipa-satellite"

Properties	
Name	RHEL7-ipa-satellite
Hostnames	
IP Addresses	
Container	redhat: 1 CPU (1 socket x 1 core), 1024 MB
Parent Host Platform	N/A
Platform Tools	N/A
Operating System	rhel_7x64

Compliance	
Status	Never Verified
History	Not Available

Power Management	
Power State	off
Last Boot Time	N/A
State Changed On	Wed Jul 06 06:14:36 UTC 2016

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4章 クラウドプロバイダー

CloudForms において、クラウドプロバイダーとは CloudForms アプライアンスに追加して、環境内のリソースの管理と対話を行うことが可能なクラウドコンピューティング環境のことです。本章では、CloudForms に追加可能な異種のクラウドプロバイダーとその管理方法について説明します。クラウドプロバイダーの多くは個別に、CloudForms に追加します。また Amazon EC2 および Azure クラウドプロバイダーは、CloudForms により自動的に検出されます。

Web インターフェースは、仮想サムネイルでクラウド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. インスタンス数
2. 管理システムソフトウェア
3. イメージ数
4. 認証ステータス

表4.1 プロバイダー認証ステータス

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。

4.1. OPENSTACK プロバイダー

4.1.1. 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にはこのユーザー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 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 では、CloudForms にアクセスして使用する全テナントのメンバーとして、**admin** を追加する必要があります。

CloudForms のテナンシーに関する詳細は、『**Deployment Planning Guide**』の「[Tenancy](#)」を参照してください。

OpenStack クラウドまたはインフラストラクチャプロバイダーを追加する場合には、**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、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。新しいクラウドテナントと対応する OpenStack テナントは、クォータ以外、リソース割り当てが全く同じとなります。テナントクォータは、CloudForms と OpenStack の間では同期されず、レポート目的でのみ利用可能です。CloudForms でクォータを管理できますが、OpenStack で作成したクォータには影響はありません。

プロバイダーの更新時に、CloudForms は OpenStack のテナント一覧の変更の有無もチェックします。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。CloudForms は、OpenStack テナントに対する変更に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 Queuing 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 『**アーキテクチャガイド**』の「[OpenStack Telemetry \(ceilometer\)](#)」のセクションを参照してください。



注記

自己署名の認証局 (CA) を使用してプロバイダーを認証するには、プロバイダーを追加する前に「[自己署名の CA 証明書の使用](#)」の手順に従い、CloudForms アプライアンスが証明書を信頼するように設定します。

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 **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

OpenStack プロバイダーにクラウドテナントを作成するには、Keystone API v3 が必要です。



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。
- 作成中のプロバイダーには、指定のドメインのプロジェクトのみが表示されます。他のドメインのプロジェクトを表示するには別のクラウドプロバイダーとしてプロジェクトを追加してください。OpenStack のドメイン管理に関する情報は、『Red Hat OpenStack Platform **Users and Identity Management Guide**』の「[Domain Management](#)」を参照してください。

6. リージョン に、リージョン番号を入力します。
7. プロバイダー用に適切な **ゾーン** を入力します。ゾーンを指定しない場合は、ゾーンは **default** に設定されます。
8. 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** に設定します。
9. 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ゾーンの定義を参照してください。

10. 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. **セキュリティープロトコル** の方法を選択して、プロバイダーの認証方法を指定します。
 - **検証なしの SSL**: SSL を使用してセキュアでない方法でプロバイダーを認証します。
 - **SSL**: 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。これは、推奨の認証方法です。
 - **非 SSL**: SSL なしの HTTP プロトコルのみでセキュアでない方法でプロバイダーに接続します。
 - b. 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。

- c. **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。
- 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** 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。
11. 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、または、Ceilometer でイベントが有効化されていない場合には、**AMQP** を選択して以下を設定します。
 - a. **セキュリティープロトコル** メソッドを選択します。
 - b. **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。
 - c. **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。
 - 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** のフィールドに入力します。
 - e. **検証** をクリックして認証情報を確認します。
12. クラウドプロバイダーを設定した後は、**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。
- OpenStack クラウドプロバイダーから容量と使用状況データを収集するには、設定メニューの**構成のすべてのクラスターの収集** オプションを選択する必要があります。詳細は、『**全般設定ガイド**』の「**容量と使用状況の収集**」を参照してください。

4.1.1.1. 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. 以下の **注記** を確認してください。

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
```

注記

新規作成した環境ファイルをオーバークラウドデプロイメントに渡す場合は、環境に左右され、使用する変数によって特定の順番にコマンドを実行する必要があります。詳細情報は、Red Hat OpenStack Platform ドキュメントの「**Director インストールと使用**」を参照してください。

4.2. AZURE プロバイダー

4.2.1. 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します。CloudForms が Microsoft Azure に対して認証できるようにするには、Azure ポータルを使用して必要な手順を踏む必要があります。「**Create Active Directory application and service principal account using the Azure portal**」を参照

してください。Azure Active Directory (Azure AD) の設定手順に従い、必要なパーミッションの割り当てて、Azure Active Directory アプリケーションを作成し、CloudForms のプロバイダーとして Azure インスタンスに追加、接続する必要がある **アプリケーション ID** (クライアント ID)、**ディレクトリー ID** (テナント ID)、**サブスクリプション ID** および **キー値** (クライアントキー) を取得します。現在、これらの手順はすべて Azure Resource Manager または Service Manager (Classic) モードを使用して実行できます。

注記

「[Create Active Directory application and service principal account using the Azure portal](#)」の記載の手順では、以下が説明されています。

- **アプリケーション ID と認証キーの取得** 時に取得した **アプリケーション ID** が **クライアント ID** となります。同じセクションで、鍵の説明と期間を指定してから、**保存** をクリックした後に表示される **値** が **クライアントキー** になります。有効期限のあるキーを選択した場合には、中断を回避できるように期限前に新しいキーを生成できるように、有効期限をメモするようにしてください。
- **テナント ID の取得** 時に取得した **ディレクトリー ID** が **テナント ID** です。Azure Active Directory (Azure AD) では、テナントは Azure AD サービスの専用のインスタンスで、組織の代表となります。組織には、社内のユーザーと、その情報 (ユーザープロファイルデータ、パーミッション、グループ、アプリケーション、組織やセキュリティ関連のその他の情報) が格納されます。Azure AD ユーザーがアプリケーションにサインインできるようにするには、テナント ID (ディレクトリー ID) が割り当てられているご自身のテナントに、アプリケーションを登録する必要があります。
- **アプリケーションのロールへの割り当て** 時に、**Reader** ロールではなく、**Contributor** ロールを選択します。
- **サブスクリプション ID** を取得するには、Azure ポータルにログインして、左側のスライドアウトメニューで **サブスクリプション** をクリックします。適切なサブスクリプションを検索して、関連付けられている Azure **サブスクリプション ID** を確認します。**サブスクリプション** タブが表示されていない場合には、**他のサービス** をクリックして検索します。Azure **サブスクリプション ID** は、仮想マシンやストレージなど、Azure アカウントで使用する全サービスの請求ユニットのようなものです。**サブスクリプション ID** はグローバル一意識別子 (GUID) の形式を使用します。



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 AD 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。

- ディレクトリー ID (テナント ID)
- サブスクリプション ID
- アプリケーション ID (クライアント ID)
- クライアントキー

以下の手順でこれらの値を使用して、Azure クラウドインスタンスをプロバイダーとして CloudForms に追加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:

1. **コンピューター → 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** 一覧からリージョンを選択します。選択したリージョンに対して、プロバイダーが作成されます。
6. **テナント ID** を入力します。
7. **サブスクリプション ID** を入力します。
8. **ゾーン** を入力します。
9. **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。
10. **追加** をクリックします。

4.2.2. 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。

4.2.3. Azure クラウドリージョンの無効化

Red Hat CloudForms では、管理者がアプライアンスサーバーで Azure クラウドリージョンを無効化することができます。この機能を使用して、特定の区分リージョンを無効にすることができます。無効にすると、新規 Azure プロバイダーを追加する時に、そのリージョンは利用できません。

1. 設定メニューから **構成** を選択します。
2. **設定** アコーディオンメニューから **ゾーン** をクリックします。
3. CloudForms サーバーが配置されるゾーンをクリックしてから、EVM サーバーをクリックします。
4. **詳細** タブをクリックします。
5. **:ems_azure:** を検索して、**:disabled_regions:** に無効にするリージョンを入力します。

Example. To disable the `us-gov-arizona` and `us-gov-texas` regions:

```

:ems_azure:
:disabled_regions:
- us-gov-arizona
- us-gov-texas

```

6. **保存** をクリックします。

4.3. AMAZON EC2 プロバイダー

4.3.1. 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)

4.3.2. Amazon EC2 プロバイダーの追加



以下の手順を実行して CloudForms に 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. **リージョン** 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. **エンドポイント** の **デフォルト** タブをクリックします。
 - a. 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。

- b. **検証** をクリックして認証情報を検証します。
8. **SmartState Docker** タブをクリックします。
 - a. **SmartState Docker ユーザー名** と **SmartState Docker パスワード** を入力します。これらの認証情報を使用して、AWS で SmartState 分析を行うのに必要な、Docker コンテナイメージのレジストリーにアクセスします。
9. **追加** をクリックします。

4.3.3. 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。

4.3.4. 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。



注記

パブリックイメージすべてを同期すると、追加のメモリーリソースが必要な場合があります。また、同期は、Amazon EC2 プロバイダーごとに同期が行われ、全メモリーリソースと同様の容量が必要となることを念頭においてください。

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。
4. オプションで **public_images_filters** でフィルターのアレイを設定して、どのイメージを同期するかを絞り込みます。詳しい情報は、http://docs.aws.amazon.com/sdkforruby/api/Aws/EC2/Client.html#describe_images-instance_method を参照してください。

4.3.5. 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

4.3.6. Amazon クラウドリージョンの無効化

Red Hat CloudForms では、管理者がアプライアンスサーバーで Amazon クラウドリージョンを無効化することができます。この機能を使用して、AWS GovCloud などの特定の区分リージョンを無効にすることができます。無効にすると、Amazon EC2 プロバイダーを追加する時に、そのリージョンは利用できません。

1. 設定メニューから **構成** を選択します。
2. **設定** アコーディオンメニューから **ゾーン** をクリックします。
3. CloudForms サーバーが配置されるゾーンをクリックしてから、EVM サーバーをクリックします。
4. **詳細** タブをクリックします。

5. `:ems_amazon:` を検索して、`:disabled_regions:` に無効にするリージョンを入力します。

Example. To disable the `ap-northeast-1` region:

```
:ems_amazon:
  :disabled_regions:
    - us-gov-west-1
    - ap-northeast-1
```

6. 保存 をクリックします。



注記

AWS では政府のリージョンはデフォルトでは無効になっています。無効なリージョンを有効化するには、`production.yml` 設定ファイルで手動で設定するようにしてください。

4.4. GOOGLE COMPUTE ENGINE プロバイダー

4.4.1. 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

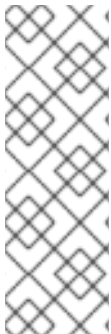
対象のプロジェクト用のプライベート JSON キーは、Google Cloud Platform の **IAM と管理** → **サービスアカウント** で生成することができます。このキーは、プロバイダーに対して認証を行う際に使用されます。

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" }
```

4.4.2. 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ログのエントリ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 ログिंग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。

4.4.2.1. 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。

Exports

Select service

Compute Engine

Export these sources

☐ All logs

compute.googleapis.com/activity_log

+ Add item

Select export destinations

Stream to BigQuery dataset ?

Don't export to BigQuery

Save to Cloud Storage bucket ?

Don't export to Cloud Storage

Publish to Cloud Pub/Sub topic ?

manageiq-activity-log

Save

Revert

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。



4.4.2.2. 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。



4.5. 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。



4.6. 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。

Tag Assignment

Select a customer tag to assign: Environment * <Select a value to assign>

Category	Assigned Value
 Cost Center *	Cost Center 001
 Environment *	Quality Assurance

* Only a single value can be assigned from these categories

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。

4.7. クラウドプロバイダーの削除

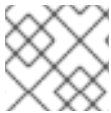
使用しなくなったクラウドプロバイダーを VMDB から削除する必要がある場合があります。

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。

4.8. 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. **コンピューター** → **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。

4.9. 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. **コンピューター** → **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5章 ネットワークマネージャー

Red Hat CloudForms において、ネットワークマネージャーとは CloudForms アプライアンスで管理される既存のクラウドおよびインフラストラクチャプロバイダー上にあるネットワークエンティティのインベントリのことです。

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**、**Google Cloud Network** 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。

本章は、CloudForms で利用可能な各種ネットワークマネージャーとその管理方法について説明します。ネットワークマネージャーは CloudForms により、他の接続プロバイダーから自動的に検出されます。

5.1. 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**、**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** 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。



5.2. 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。



5.3. 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。



5.4. 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。

5.5. 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。

5.6. 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

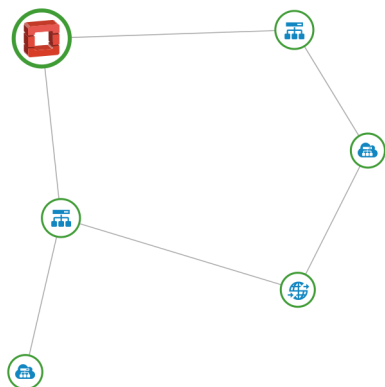
トポロジーウィジェットは、Red Hat CloudForms がアクセス可能なネットワークプロバイダーの異なるエンティティー間のステータスとリレーションシップを表示する、インタラクティブなトポロジーグラフです。

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。

☐ Display Names

Cloud Subnets VMs Security Groups Floating Ips Cloud Networks Network Routers Cloud Tenants Tags



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** をクリックすると、トポロジ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6章 ミドルウェア管理プロバイダー

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とそれらの管理方法について説明します。

ミドルウェアプロバイダーは、CloudForms の管理機能を、管理仮想マシン、ホスト、および Linux コンテナで実行中の JBoss Middleware アプリケーションコンテナに拡張します。プロバイダーは、インベントリ、イベント、メトリック、および電源操作を提供します。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

今回のリリースのミドルウェアプロバイダーはテクノロジープレビューです。テクノロジープレビューでは、今後の製品イノベーションを早い段階で利用できるので、新機能をテストして、開発プロセス時にフィードバックを提供することができます。テクノロジープレビューは実稼働環境での使用を目的としていません。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、[「テクノロジープレビュー機能のサポート範囲」](#)を参照してください。

6.1. ミドルウェア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、ミドルウェアプロバイダーをアプライアンスに追加します。



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. Middleware Manager など、プロバイダーの **名前** を入力します。
4. **タイプ** の一覧から **Hawkular** を選択します。
5. デフォルトの **ゾーン** を受け入れます。
6. **エンドポイント** でミドルウェアプロバイダーの以下の情報を設定します。
 - a. **セキュリティープロトコル** メソッドを選択して、プロバイダーへの認証方法を指定します。プロバイダーの認証に SSL を使用するには、**HAWKULAR_USE_SSL=true** のサービスオプションを使用して、ミドルウェア管理サーバーを起動しておく必要があります。



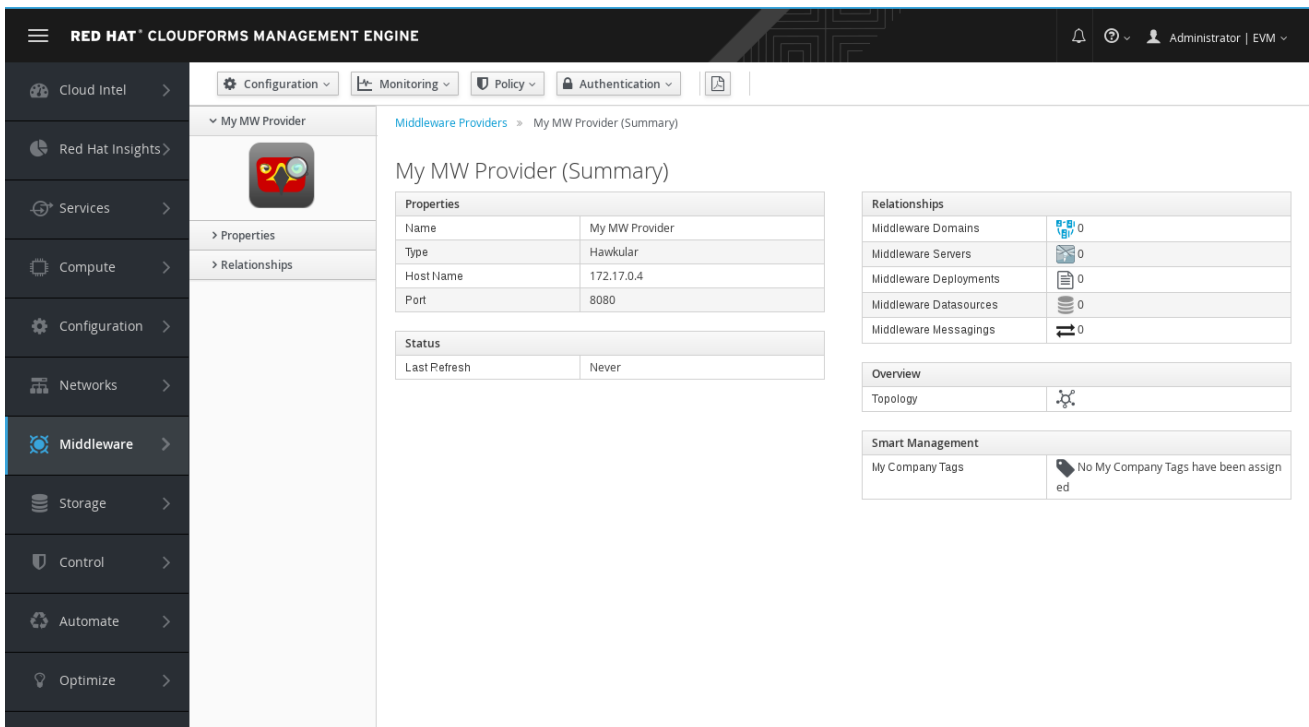
注記

Hawkular の現在のリリースが唯一サポートするセキュリティープロトコルは、**検証なしの SSL** と **SSL なし** だけです。

- **SSL (認証あり)**: 信頼済みの認証局を称してセキュアにプロバイダーを認証します。これには、PEM ファイルまたは単一の .pkcs12 ファイルで **/client-secrets** ディレクトリーに公開鍵と秘密鍵をあらかじめ設定しておく必要があります。

- **SSL の信頼されたカスタム CA:** 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、証明書の文字を .PEM 形式の **信頼された CA 証明書** フィールドにコピーします。
 - **検証なしの SSL:** セキュアでない方法でプロバイダーを認証します (非推奨)。
 - **非 SSL:** SSL を使用しない場合は選択します。
- b. ミドルウェアプロバイダーをインストールするマシンの **ホスト名** か、IPv4 または IPv6 アドレスを入力します。
 - c. ミドルウェアマネージャーの **API ポート** を入力します。デフォルトでは、8080 を使用します。
 - d. 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** を入力します。これは、**HAWKULAR_USERNAME** と一致するようにしてください。
 - e. ミドルウェアマネージャーの起動に使用する **パスワード** を入力します。これは、**HAWKULAR_PASSWORD** と一致するようにしてください。
 - f. **パスワードの確認** フィールドに、パスワードをもう一度入力します。
 - g. **検証** をクリックしてユーザーが適切な認証情報を使用していることを確認します。
7. **追加** をクリックします。
8.  (**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。




The screenshot shows the Red Hat CloudForms Management Engine interface. The left sidebar contains a navigation menu with the following items: Cloud Intel, Red Hat Insights, Services, Compute, Configuration, Networks, **Middleware** (selected), Storage, Control, Automate, and Optimize. The main content area displays the 'My MW Provider (Summary)' page. The page has a top navigation bar with tabs for Configuration, Monitoring, Policy, Authentication, and a search icon. Below the tabs, there is a breadcrumb trail: Middleware Providers > My MW Provider (Summary). The main content area is divided into several sections:

- My MW Provider (Summary)**: A summary card showing the provider's name, type, host name, port, and status.
- Properties**: A table listing the provider's properties.
- Status**: A table showing the provider's status.
- Relationships**: A table showing the provider's relationships with other resources.
- Overview**: A section showing the provider's topology.
- Smart Management**: A section showing the provider's management status.

Properties	
Name	My MW Provider
Type	Hawkular
Host Name	172.17.0.4
Port	8080

Status	
Last Refresh	Never

Relationships	
Middleware Domains	0
Middleware Servers	0
Middleware Deployments	0
Middleware Datasources	0
Middleware Messagings	0

Overview	
Topology	

Smart Management	
My Company Tags	No My Company Tags have been assigned

第7章 コンテナプロバイダー

コンテナプロバイダーとは、コンテナ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。

Red Hat CloudForms は、OpenShift コンテナプロバイダーに接続して、インフラストラクチャーおよびクラウドプロバイダーなどと同様にこれらを管理できます。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

CloudForms は、コンテナ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)
- 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エンティティーはすべてタグ付けすることが可能です。

CloudForms ユーザーインターフェースは、仮想サムネイルでコンテナ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. ノード数
2. コンテナプロバイダーのソフトウェア
3. 電源状態
4. 認証ステータス

表7.1 コンテナプロバイダー認証ステータス

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。

7.1. OPENSIFT CONTAINER PLATFORM MANAGEMENT トークンの取得

openshift-ansible-3.0.20 (以降) を使用して OpenShift をデプロイする場合に、Red Hat CloudForms で必要とされる OpenShift Container Platform [service account](#) および [roles](#) はデフォルトでインストールされます。



注記

デフォルトのロール一覧については「[OpenShift Container Platform documentation](#)」を参照してください。

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 Container Platform のバージョンに対応するステップに従ってください。

7.1.1. OpenShift Container Platform 3.3 以降での管理トークンの取得

OpenShift Container Platform 3.3 (以降) のプロバイダーを追加するのに必要なトークンを取得するには以下を実行します。

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

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

OpenShift Container Platform 3.2 のプロバイダーを追加するのに必要なトークンを取得するには以下を実行します。

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

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

OpenShift Container Platform 3.1 のプロバイダーを追加するのに必要なトークンを取得するには以下を実行します。

1. 以下を実行して、**management** サービスアカウントのトークン名を取得します。

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

2. 完全なトークンの出力を取得するには、トークンの 1 つを選択して記述します。**management-admin-token-0f3fh** はトークンの名前に置き換えてください。

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



7.2. OPENSIFT CLUSTER メトリックの有効化

OpenShift Cluster メトリックのプラグインを使用してノード、ポッド、コンテナのメトリックを 1 つの場所に収集します。これにより、使用状況を追跡して共通の問題を特定します。

- Red Hat CloudForms がすべて 3 つの [容量 & 使用状況 サーバーロール](#) を使用できるように設定します。
- [OpenShift Container Platform ドキュメント](#) を使用してクラスターのメトリックを有効化します。

7.3. OPENSIFT CONTAINER PLATFORM 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 Container Platform Management トークンの取得](#)」で取得したトークンを使用して以下の手順に従い、OpenShift Container Platform プロバイダーを追加します。

1. コンピュート → コンテナ → 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 Container Platform** 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。ゾーンを指定しない場合は、ゾーンは **default** に設定されます。
6. **アラート** 一覧から **Prometheus** を選択して、外部アラートを有効にします。**Prometheus** を選択すると、Prometheus サービスを設定するために、下部のペインに **Alerts** タブが追加されます。アラートはデフォルトでは無効になっています。
7. **メトリック** 一覧から **Hawkular** または **Prometheus** を選択して、容量および使用状況データを収集するか、**無効** のままにします。**Prometheus** または **Hawkular** を選択すると、詳細設定用

の下部のペインに **Metrics** タブが追加されます。メトリックはデフォルトでは無効になっています。

8. デフォルト タブで、OpenShift プロバイダーの以下の内容を設定します。

a. セキュリティープロトコル の方法を選択して、プロバイダーの認証方法を指定します。

- **SSL:** 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。
- **SSL の信頼されたカスタム CA:** 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、プロバイダーの CA 証明書を .PEM 形式の **信頼された CA 証明書** ボックスにコピーします。



注記

全エンドポイント (デフォルト、メトリック、アラート) の OpenShift Container Platform プロバイダーの CA 証明書は `/etc/origin/master/ca.crt` から取得できます。出力 (-----BEGIN CERTIFICATE----- で始まるブロック) を **信頼された CA 証明書** フィールドに貼り付けます。

- **検証なしの SSL:** セキュアでない方法でプロバイダーを認証します (非推奨)。

b. プロバイダーの ホスト名 (か、IPv4 または IPv6 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。

c. プロバイダーの API ポート を入力します。デフォルトのポートは **8443** です。

d. トークン ボックスでプロバイダーのトークンを入力します。



注記

プロバイダーのトークンを取得するには、プロバイダー上で `oc get secret` コマンドを実行します。詳細は、[「Obtaining an OpenShift Container Platform Management Token」](#) を参照してください。

以下に例を示します。

```
# oc get secret --namespace management-infra management-admin-token-8ixxs --template='{{index .data "ca.crt"}}' | base64 --decode
```

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

9. メトリックサービスを選択した場合には、メトリック タブでサービスの詳細を設定します。

a. セキュリティープロトコル メソッドを選択して、サービスの認証方法を指定します。

- **SSL:** 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。
- **SSL の信頼されたカスタム CA:** 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、プロバイダーの CA 証明書を .PEM 形式の **信頼された CA 証明書** ボックスにコピーします。



注記

OpenShift では、ルーターをデフォルトでデプロイメントすると、インストール時に証明書が生成され、この証明書を **SSL trusting custom CA** オプションで使うことができます。このオプションで Hawkular エンドポイントを接続する場合は、クラスターがサービス証明書に使用する CA 証明書が必要です。このサービス証明書は、クラスターの最初のマスター上の `/etc/origin/master/service-signer.crt` に保存されます。

- **検証なしの SSL:** SSL を使用してセキュアでない方法でプロバイダーを認証します (推奨ではありません)。
- プロバイダーの **ホスト名** (か、IPv4 または IPv6 アドレス) を入力するか、**検出** ボタンを使用してホスト名を検索します。
 - Hawkular 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。デフォルトのポートは **443** です。
 - 検証** をクリックして、Red Hat CloudForms がメトリックエンドポイントに接続できることを確認します。
10. **Prometheus** アラートサービスの場合は、**Alerts** タブに Prometheus アラートエンドポイントを追加します。
- セキュリティープロトコル** メソッドを選択して、サービスの認証方法を指定します。
 - **SSL:** 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。
 - **SSL の信頼されたカスタム CA:** 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、プロバイダーの CA 証明書を .PEM 形式の **信頼された CA 証明書** ボックスにコピーします。
 - **検証なしの SSL:** SSL を使用してセキュアでない方法でプロバイダーを認証します (推奨ではありません)。
 - ホスト名** (または IPv4/IPv6 アドレス) か、アラート **ルート** を入力します。
 - Prometheus 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。デフォルトのポートは **443** です。
 - 検証** をクリックして、CloudForms がアラートサービスに接続できることを確認します。
11. **詳細** タブをクリックして、OpenSCAP を使用してプロバイダー上のコンテナイメージをスキャンするイメージインスペクター設定を追加します。



注記

これらの設定により、イメージインスペクターのコンテナイメージをレジストリーからダウンロードして、(効率的にスキャンできるように) プロキシ経由で Common Vulnerabilities and Exposures (CVE) の情報を取得します。

- a. **HTTP、HTTPS** および **NO Proxy** にプロバイダーのプロキシ情報を入力します。
- b. **Image-Inspector Repository** 情報を入力します。
- c. **Image-Inspector Registry** 情報を入力します。
- d. **Image-Inspector Tag** の値を入力します。タグは、リポジトリでイメージを区別するために使用するマークで、通常、イメージに保存するアプリケーションのバージョンで区別されます。
- e. **CVE location** を入力します。

12. **追加** をクリックします。



注記



個別のプロバイダー設定ではなく、全 OpenShift プロバイダーのグローバルデフォルトのイメージインスペクター設定も、**ems_kubernetes** の値を編集することで、詳細設定メニューから指定できます。

以下に例を示します。

```
:image_inspector_registry: registry.access.redhat.com
:image_inspector_repository: openshift3/image-inspector
```



7.4. コンテナ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. **コンピューター → コンテナ → プロバイダー** に移動します。
2. タグ付けするコンテナ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。

Tag Assignment

Select a customer tag to assign: Environment * <Select a value to assign> *



	Category	Assigned Value
	Cost Center *	Cost Center 001
	Environment *	Quality Assurance

* Only a single value can be assigned from these categories

5. 割り当てる値を選択します。
6. **保存** をクリックします。

7.5. コンテナプロバイダーの削除

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

1. **コンピューター** → **コンテナ** → **プロバイダー** に移動します。
2. 削除するコンテナ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。

7.6. コンテナプロバイダーの一時停止/再開



CloudForms では、コンテナプロバイダーの一時停止、再開ができます。これにより、ユーザーはリソースを集中的に使用する可能性のあるプロバイダーの数を追加して、特定の時間に必要のないプロバイダーを一時停止して再開することができます。さらに、プロバイダーでメンテナンスを実行時には、CloudForms がプロバイダーに接続できないようにプロバイダーを一時停止して、ログエラーの生成や部分的なデータの収集を回避します。





注記

- プロバイダーが一時停止している場合は、プロバイダーからデータは収集されません。これにより、インベントリー、メトリック、イベントで差異が発生する可能性があります。
- また、プロバイダー自体は一時停止中にはオフになりませんが、CloudForms とプロバイダー間のリンクを一時的に無効にします。プロバイダーを再開すると、CloudForms とプロバイダー間のリンクが再度有効化されます。

コンテナプロバイダーを一時停止する手順:



1. **コンピューター** → **コンテナ** → **プロバイダー** に移動します。
2. 一時停止するコンテナプロバイダーをクリックします。
3.  (**構成**) をクリックして、 (**コンテナプロバイダーの一時停止**) をクリックします。
4. **OK** をクリックします。

一時停止したコンテナプロバイダーを再開する手順:

1. **コンピューター** → **コンテナ** → **プロバイダー** に移動します。
2. 一時停止していたコンテナプロバイダーで再開するものをクリックします。
3.  (**構成**) をクリックして、 (**このコンテナプロバイダーの再開**) をクリックします。
4. **OK** をクリックします。

7.7. コンテナプロバイダーの編集

必要に応じて、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。CloudForms 環境を以前のバージョンからアップグレードしたばかりであれば、プロバイダーを編集して、プロバイダーが Red Hat CloudForms への接続に使用する認証メソッドを指定します。

1. コンピュート → コンテナ → プロバイダー に移動します。
2. 編集するコンテナプロバイダーをクリックします。
3.  (構成) をクリックして、 (選択したコンテナプロバイダーの編集) を選択します。
4. 必要に応じて **名前** を編集します。



注記

タイプ の値は変更できません。

5. デフォルト タブの **エンドポイント** で、必要に応じて以下を編集します。
 - a. **セキュリティープロトコル** の方法を選択して、プロバイダーの認証方法を指定します。
 - **SSL**: 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。
 - **SSL の信頼されたカスタム CA**: 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、プロバイダーの CA 証明書を .PEM 形式の **信頼された CA 証明書** ボックスにコピーします。



注記

全エンドポイント (デフォルト、メトリック、アラート) の OpenShift Container Platform プロバイダーの CA 証明書は `/etc/origin/master/ca.crt` から取得できます。出力 (-----
BEGIN CERTIFICATE----- で始まるブロック) を **信頼された CA 証明書** フィールドに貼り付けます。

- **検証なしの SSL**: セキュアでない方法でプロバイダーを認証します (非推奨)。
- b. プロバイダーの **ホスト名** (か、IPv4 または IPv6 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。

- c. プロバイダーの **API ポート** を入力します。デフォルトのポートは **8443** です。
- d. **トークン** ボックスでプロバイダーのトークンを入力します。



注記

プロバイダーのトークンを取得するには、プロバイダー上で **oc get secret** コマンドを実行します。詳細は、[「Obtaining an OpenShift Container Platform Management Token」](#) を参照してください。

以下に例を示します。

```
# oc get secret --namespace management-infra management-admin-token-8ixxs --template='{{index .data "ca.crt"}}' | base64 --decode
```

- e. **検証** をクリックして、Red Hat CloudForms が OpenShift Container Platform プロバイダーに接続できることを確認します。
6. **メトリック タブの エンドポイント** で、選択した内容に応じて、Hawkular または Prometheus の容量および使用状況のメトリック収集に関する以下の項目を設定します。
 - a. **セキュリティープロトコル** の方法を選択して、プロバイダーの認証方法を指定します。
 - **SSL**: 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。
 - **SSL の信頼されたカスタム CA**: 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、プロバイダーの CA 証明書を .PEM 形式の **信頼された CA 証明書** ボックスにコピーします。
 - **検証なしの SSL**: SSL を使用してセキュアでない方法でプロバイダーを認証します (推奨ではありません)。
 - b. プロバイダーの **ホスト名** (か、IPv4 または IPv6 アドレス) を入力します。
 - c. 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。デフォルトのポートは **443** です。
 - d. **検証** をクリックして、Red Hat CloudForms がエンドポイントに接続できることを確認します。
 7. **アラート タブの エンドポイント** で、クラスターからの Prometheus アラートに関する以下の内容を設定します。
 - **SSL**: 信頼済みの認証局を使用してセキュアにプロバイダーを認証します。プロバイダーに有効な SSL 証明書があり、信頼済みの認証局により署名されている場合にはこのオプションを選択します。このオプションでは、他の設定は必要ありません。
 - **SSL の信頼されたカスタム CA**: 自己署名済みの証明書でプロバイダーを認証します。このオプションでは、プロバイダーの CA 証明書を .PEM 形式の **信頼された CA 証明書** ボックスにコピーします。
 - **検証なしの SSL**: SSL を使用してセキュアでない方法でプロバイダーを認証します (推奨ではありません)。
 - a. プロバイダーの **ホスト名** (か、IPv4 または IPv6 アドレス) を入力します。
 - b. 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。デフォルトのポートは **443** です。

- c. **検証** をクリックして、Red Hat CloudForms がエンドポイントに接続できることを確認します。

- 8. **保存** をクリックします。

7.8. コンテナプロバイダーの環境変数の非表示

ユーザーロールを設定して、コンテナプロバイダーの環境変数をユーザーに表示されないように制限することができます。

これは、パスワードなどの機密情報が環境変数パネルには公開されるので、特定のユーザーに表示しない場合などに便利です。







注記

CloudForms のデフォルトのユーザーロールは読み取り専用です。ロールの設定をカスタマイズするには、新規ロールを作成するか、既存のロールのコピーを作成してください。

アクセス制御 のロールをクリックして、そのロールがアクセスできるロール情報や製品の機能 (チェックマークで印付け) を表示できます。**製品機能** のカテゴリーを展開して、詳細を表示します。

コンテナの環境変数に対するユーザーアクセスを設定する手順:

1. 設定メニューから **構成** を選択します。
2. **アクセス制御** アコーディオンメニューから **ロール** をクリックします。
3. **アクセス制御ロール** 一覧から既存のカスタムロールを選択して、 (**構成**) をクリックし、 (**選択したロールの編集**) をクリックします。
または、新規カスタムロールを作成するには、**アクセス制御ロール** 一覧からロールを選択して、 (**構成**) をクリックし、 (**新規ロールへのこのロールのコピー**) をクリックします。
4. 任意でロールの名前を編集します。
5. **サービス、仮想マシン、およびテンプレートのアクセス制限** では、このロールが指定されているユーザーに対して表示する内容を、このユーザーまたはグループが所有するリソースのみ、またはユーザーが所有するリソースのみに制限するのか、全リソースにするのかを選択します (**None**)。
6. **製品機能 (編集)** のツリーオプションを展開して、**すべて** → **コンピュー** → **コンテナ** → **コンテナエクスプローラー** → **すべてのコンテナ** → **コンテナの表示** を表示します。
7. **環境変数** のチェックボックスのチェックを外して、対象のユーザーロールにコンテナ環境変数を表示しないように制限します。

Role Information

Name

Access Restriction for Services, VMs, and Templates

Product Features (Editing)

- ✓ ☒ Everything
 - > ☒ Cloud Intel
 - > ☐ Red Hat Insights
 - > ☐ Services
 - ✓ ☒ Compute
 - > ☒ Clouds
 - > ☒ Infrastructure
 - > ☐ Physical Infrastructure
 - ✓ ☒ Containers
 - > ☒ Containers Dashboard
 - > ☒ Container Providers
 - > ☒ Projects
 - > ☒ Routes
 - > ☒ Services
 - > ☒ Replicators
 - > ☒ Pods
 - ✓ ☒ Containers Explorer
 - > ☒ Relationships
 - ✓ ☒ All Containers
 - ✓ ☒ View Containers
 - ☒ List
 - ☒ Timeline
 - ☒ Environment Variables
 - > ☐ Modify
 - > ☒ Operate
 - > ☒ Nodes



Save Reset Cancel

8. 保存 をクリックします。

ユーザーロールの詳細情報は、『設定全般』の「[ロール](#)」を参照してください。

7.9. コンテナプロバイダーのタイムラインの表示

コンテナ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 → 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。

詳細情報については各項目をクリックします。

7.10. コンテナの概要のページ

コンピューター → コンテナ → オブジェクト の順に移動して、多くの異なるコンテナオブジェクトの情報を表示します。

7.10.1. 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 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 Container Platform Installation and Configuration Guide](#)』ガイドを参照して、希望の OpenShift バージョンを使用していることを確認します。

7.10.2. コンテナ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プロバイダーおよびエンティティについての情報は、コンテナの **概要** ページに要約されます。**概要** のページでは、コンテナプロバイダーおよびエンティティ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。

1 Providers	1 Nodes	21 Containers	2 Registries	12 Projects
1	22 Pods	15 Services	10 Images	11 Routes

コンテナ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 → **概要** に移動します。
2. 必要なコンテナのエンティティ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。

7.10.2.1. オブジェクトの概要の表示

オブジェクトの概要へは コンピュート → コンテナ → <オブジェクト> の順で移動し、このページではオブジェクト数の情報やそのコンポーネントを表示することができます。

コンテナプロバイダーの概要の表示

コンピュート → コンテナ → プロバイダー の順に移動して、コンテナプロバイダーの異なる面に関する情報を表示します。概要には以下が含まれます。

- プロバイダーとそのコンポーネントのステータス
- コンテナプロバイダーの異なるエンティティ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。

RED HAT® CLOUDFORMS MANAGEMENT ENGINE



Relationships	
Projects	6
Routes	3
Services	6
Replicators	4
Pods	8
Containers	5
Nodes	2
Image Registries	1
Images	5

Overview	
Topology	

Smart Management	
Managed by Zone	default
My Company Tags	No My Company Tags have been assigned

- 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

コンテナノードの概要の表示

コンピューター → コンテナ → プロバイダー の順に移動して、コンテナノードの異なる面に関する情報を表示します。概要には以下が含まれます。

- ノード上のエンティティー数
- ノードの容量と使用状況
- 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

コンテナノードの概要ページからノードのイベントのタイムラインを表示するには、 (監視) をクリックして、 (タイムライン) 選択します。

コンテナの概要の表示

コンピューター → コンテナ → コンテナ の順に移動して、コンテナの異なる面に関する情報を表示します。概要には以下が含まれます。

コンテナ → コンテナノード → プロバイダー → プロバイダーの概要

- コンテナーと関連するノート/ホスト/イメージとの関係
- コンテナーが実行されているノード
- コンテナーの ID
- 名前、タグなどのコンテナーイメージのプロパティ

コンテナーイメージの概要の表示

コンピューター → コンテナー → コンテナーイメージ の順に移動して、コンテナーイメージの異なる面に関する情報を表示します。概要には以下が含まれます。

- 現在このイメージを使用するコンテナー
- イメージのソースとなるイメージレジストリー

イメージレジストリーの概要の表示

コンピューター → コンテナー → イメージレジストリー の順に移動して、イメージレジストリーの異なる面に関する情報を表示します。概要には以下が含まれます。

- どのイメージがレジストリーをベースとしているか
- このレジストリーをベースとするイメージ数
- このレジストリーからのイメージを使用するコンテナー
- レジストリーのホストとポート

ポッドの概要の表示

コンピューター → コンテナー → ポッド の順に移動して、ポッドの異なる面に関する情報を表示します。概要には以下が含まれます。

- ポッドに属するコンテナー
- ポッドを参照するサービス
- ポッドが実行されるノード
- 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

レプリケーターの概要の表示

コンピューター → コンテナー → レプリケーター の順に移動して、レプリケーターの異なる面に関する情報を表示します。概要には以下が含まれます。

- 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クター

コンテナーサービスの概要の表示

コンピューター → コンテナ → コンテナ の順に移動して、コンテナサービスの異なる面に関する情報を表示します。概要には以下が含まれます。

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

ボリュームの概要の表示

コンピューター → コンテナ → ボリューム の順に移動して、コンテナプロバイダーの永続ボリュームに関する情報を表示します。概要には以下が含まれます。

- 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)

コンテナビルドの概要の表示

コンピューター → コンテナ → コンテナビルド の順に移動して、コンテナビルドの異なる面に関する情報を表示します。概要には以下が含まれます。

- そのコンテナ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

コンテナテンプレートの概要表示

コンピューター → コンテナ → コンテナテンプレート の順に移動して、コンテナテンプレートの異なる面に関する情報を表示します。概要には以下が含まれます。

- 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

7.10.3. 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プロバイダーおよびプロジェクト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、全コンテナのプロバイダー環境内のポッド、コンテナ、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。

7.10.3.1. コンテナプロバイダーのトポロジーの表示

1. コンピュート → コンテナ → 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。

7.10.3.2. コンテナプロバイダープロジェクトのトポロジーの表示

プロジェクトトポロジーページは、関連のエンティティが周りにある中央ノードとしてプロジェクトを表示します。

1. コンピュート → コンテナ → プロジェクト の順に移動します。
2. プロジェクトをクリックします。
3. プロジェクトの概要ページの右上にある  (トポロジービュー) をクリックします。



7.10.3.3. トポロジービューに表示するコンテナ数の制限

1. 設定メニューから **マイ設定** に移動して、**表示** タブをクリックします。
2. **デフォルトのトポロジービューで表示される項目** でドロップダウンからコンテナの項目数を選択します。
3. **保存** をクリックします。

7.10.4. SmartState 分析の実行

コンテナイメージの 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 → コンテナイメージ に移動します。
2. 分析するコンテナ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8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、Red Hat CloudForms への追加方法を説明します。

以下は、Red Hat CloudForms で現在利用可能なストレージマネージャー 3 つのタイプです。

- Amazon Elastic Block Store
- OpenStack Block Storage (**openstack-cinder**)
- OpenStack Object Storage (**openstack-swift**)

8.1. AMAZON ELASTIC BLOCK STORE マネージャー

Amazon Elastic Block Store サービスは、Amazon EC2 instances が消費可能な永続ブロックストレージリソースを提供、管理します。

Amazon Elastic Block Store サービスをストレージマネージャーとして使用するには、まず Amazon EC2 クラウドプロバイダーを Red Hat CloudForms アプライアンスに追加する必要があります。Amazon Elastic Block Store サービスは Red Hat CloudForms により自動検出され、ストレージマネージャー一覧に追加されます。Amazon EC2 クラウドプロバイダーの追加に関する説明は「[Amazon EC2 プロバイダーの追加](#)」を参照してください。



注記

Amazon Elastic Block Store マネージャーで利用可能なインベントリーを管理する方法については、『[インフラストラクチャーおよびインベントリーの管理](#)』ガイドの「[ボリューム](#)」を参照してください。

8.2. OPENSTACK BLOCK STORAGE マネージャー

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。Red Hat 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。



注記

OpenStack Block Storage マネージャーで利用可能なインベントリーを管理する方法については、『[インフラストラクチャーおよびインベントリーの管理](#)』ガイドの「[ボリューム](#)」を参照してください。

8.3. 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。Red Hat 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。

8.3.1. 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。

付録A 付録

A.1. 自己署名の CA 証明書の使用

SSL 認証用に自己署名の証明局 (CA) の証明書を追加する場合は、OpenStack Platform および Microsoft System Center Virtual Machine Manager (SCVMM) プロバイダーに対する追加設定が必要です。



注記

ユーザーインターフェースで **セキュリティープロトコル** として **SSL の信頼されたカスタム CA** を選択するオプションがある OpenShift Container Platform、Red Hat Virtualization、ミドルウェアマネージャープロバイダーを使用する場合は、以下の手順は必要ありません。これらの手順は、ユーザーインターフェースにこのオプションのないプロバイダーに対してのみ必要です。

プロバイダーを追加する前に以下を設定します。

1. PEM 形式のプロバイダーの CA 証明書を、CloudForms アプライアンスの **/etc/pki/ca-trust/source/anchors/** にコピーします。
2. アプライアンスでのトラストの設定を更新します。

```
# update-ca-trust
```

3. サーバーで EVM プロセスを再起動します。

```
# rake evm:restart
```

CA 証明書がアプライアンスに追加され、このプロバイダーを CloudForms に追加できるようになります。