Red Hat Satellite 6.2

サーバー管理ガイド

Red Hat Satellite 6 Server の管理

エディッション 1.0

Last Updated: 2018-05-04

Red Hat Satellite 6.2 サーバー管理ガイド

Red Hat Satellite 6 Server の管理
エディッション 1.0

Red Hat Satellite Documentation Team
satellite-doc-list@redhat.com

法律上の通知

概要

『Red Hat Satellite 6 Server 管理ガイド』では、Red Hat Satellite 6 Server を設定および管理する手順について説明します。この作業を続行する前に、Red Hat Satellite 6 Server と必要なすべての Capsule Server が正常にインストールされている必要があります。

目次

第1章 RED HAT SATELLITE へのアクセス

1.1. RED HAT SATELLITE　へのログイン

Red Hat Satellite のインストールと設定が終わったら、Web ユーザーインターフェースを使用して Satellite にログインし、追加の設定を行います。

手順1.1 Katello ルート CA 証明書のインストール

初めて Satellite にログインする場合は、デフォルトの自己署名証明書を使用していることを通知する警告が表示されることがあります。また、適切なルート CA 証明書がブラウザーにインストールされるまでこのブラウザーを Satellite に接続できないことがあります。以下の手順を実行して、Satellite サーバー上でルート CA 証明書を特定し、ブラウザーにインストールします。

1. **http://*HOSTNAME*/pub** を参照します。
2. *katello-server-ca.crt* を選択します。
3. 証明書をブラウザーにインポートします。

手順1.2 Satellite へのログイン:

1. Web ブラウザーで以下のアドレスを使用して Satellite Server にアクセスします。

   https://*HOSTNAME*/

   ホスト名を確認するには、プロンプトで **hostname** コマンドを使用します。

   ```
   # hostname
   ```

重要

Satellite に初めてアクセスする場合は、Web ブラウザーに信頼できない接続を警告するメッセージが表示されます。自己署名証明書を承認し、Satellite の URL をセキュリティー例外に追加し、設定を上書きします。この手順は、使用しているブラウザーによって異なる場合があります。

この操作は、Satellite の URL が信頼できるソースであることを確認できる場合にのみ実行してください。

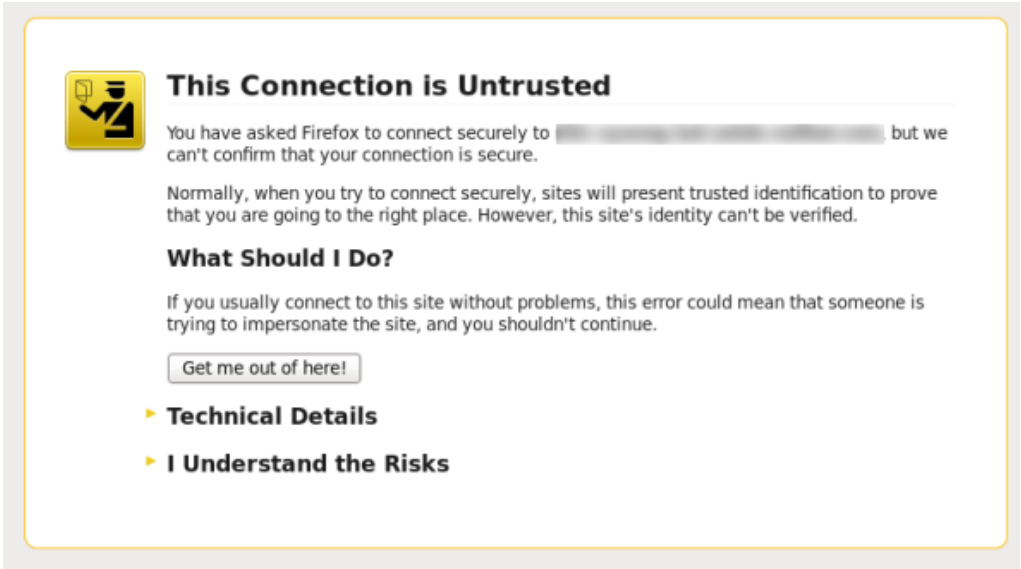


図1.1 信頼できない接続についての警告

2. 設定プロセスで作成したユーザー名とパスワードを入力します。設定時にユーザーが作成されなかった場合、デフォルトのユーザー名は **admin** になります。

結果:

正常にログインすると、Satellite ダッシュボードに移動します。ダッシュボードには、Satellite と登録されたホストの概要が表示されます。

主なナビゲーションタブは以下のとおりです。

表1.1 ナビゲーションタブ

ナビゲーションタブ	説明
Default Organization（デフォルト組織）	このタブをクリックすると、組織とロケーションが変更されます。組織やロケーションが選択されていない場合、デフォルト組織は **任意の組織** に、デフォルトロケーションは **任意のロケーション** になります。このタブを使用して異なる値に変更します。
モニター	概要のダッシュボードおよびレポートを表示します。
コンテンツ	コンテンツ管理ツールを提供します。コンテンツビュー、アクティベーションキー、ライフサイクル環境などが含まれます。
コンテナー	コンテナー管理ツールを提供します。

ナビゲーションタブ	説明
ホスト	ホストインベントリーおよびプロビジョニング設定ツールを提供します。
設定	一般的な設定ツール、およびホストグループや Puppet データを含むデータを提供します。
インフラストラクチャー	Satellite 6 が環境と対話する方法を設定するツールを提供します。
Red Hat Insights	Red Hat Insights 管理ツールを提供します。
管理	一般設定のほかに、ユーザーおよび RBAC 設定などの詳細設定を提供します。
任意のユーザー名	ユーザーが個人情報を編集できるユーザー管理機能を提供します。

注記

管理パスワードを忘れた場合は、Satellite コマンドラインインターフェースにログオンして、管理ユーザーとパスワードをリセットします。

```
# foreman-rake permissions:reset
Reset to user: admin, password: qwJxBptxb7Gfcjj5
```

これにより、デフォルトユーザー **admin** のパスワードがコマンドラインに出力されたパスワードに再設定されます。セキュリティー関連の問題が発生しないように、ログイン時にこのパスワードを変更してください。

1.2. RED HAT SATELLITE でパスワードを変更する

以下の手順は、パスワードを変更する方法について説明しています。

手順1.3 Red Hat Satellite パスワードの変更:

1. 右上にあるユーザー名をクリックします。
2. メニューから **ユーザーのアカウント** を選択します。
3. **Password (パスワード)** フィールドに新しいパスワードを入力します。
4. **Verify (検証)** フィールドに新しいパスワードを再入力します。
5. **送信** ボタンをクリックして新しいパスワードを保存します。

第2章 RED HAT SATELLITE の起動および停止

Satellite は、コマンドラインから Satellite サービスを管理するために **katello-service** コマンドを提供します。このコマンドは Satellite をアップグレードする場合やバックアップを作成する場合に役に立ちます。これらのユースケースの詳細については、Red Hat Satellite Installation Guide を参照してください。

satellite-installer コマンドを使用して Satellite をインストールしたあとに、すべての Satellite サービスは自動的に起動され有効になります。これらのサービスのリストを表示するには、以下のコマンドを実行します。

```
# katello-service list
```

実行中のサービスのステータスを確認するために、以下のコマンドを実行します。

```
# katello-service status
```

すべての Satellite サービスを停止するために、以下のコマンドを実行します。

```
# katello-service stop
```

すべての Satellite サービスを起動するために、以下のコマンドを実行します。

```
# katello-service start
```

すべての Satellite サービスを再起動するために、以下のコマンドを実行します。

```
# katello-service restart
```

第3章 組織、ロケーション、およびライフサイクル環境の設定

Red Hat Satellite 6 では、組織とロケーションの管理が統一されました。システム管理者は 1 つの Satellite Server で複数の組織とロケーションを定義します。たとえば、3 つの組織 (財務、マーケティング、および営業) が 3 つの国 (アメリカ、イギリス、および日本) に存在する会社があるとします。この場合、Satellite Server はシステムを管理する 9 つのコンテキストを作成してすべてのロケーションのすべての組織を管理します。また、ユーザーは特定のロケーションを定義し、ネストして階層を作成できます。たとえば、Satellite 管理者はアメリカをボストン、フェニックス、サンフランシスコなどの特定の都市に分割できます。

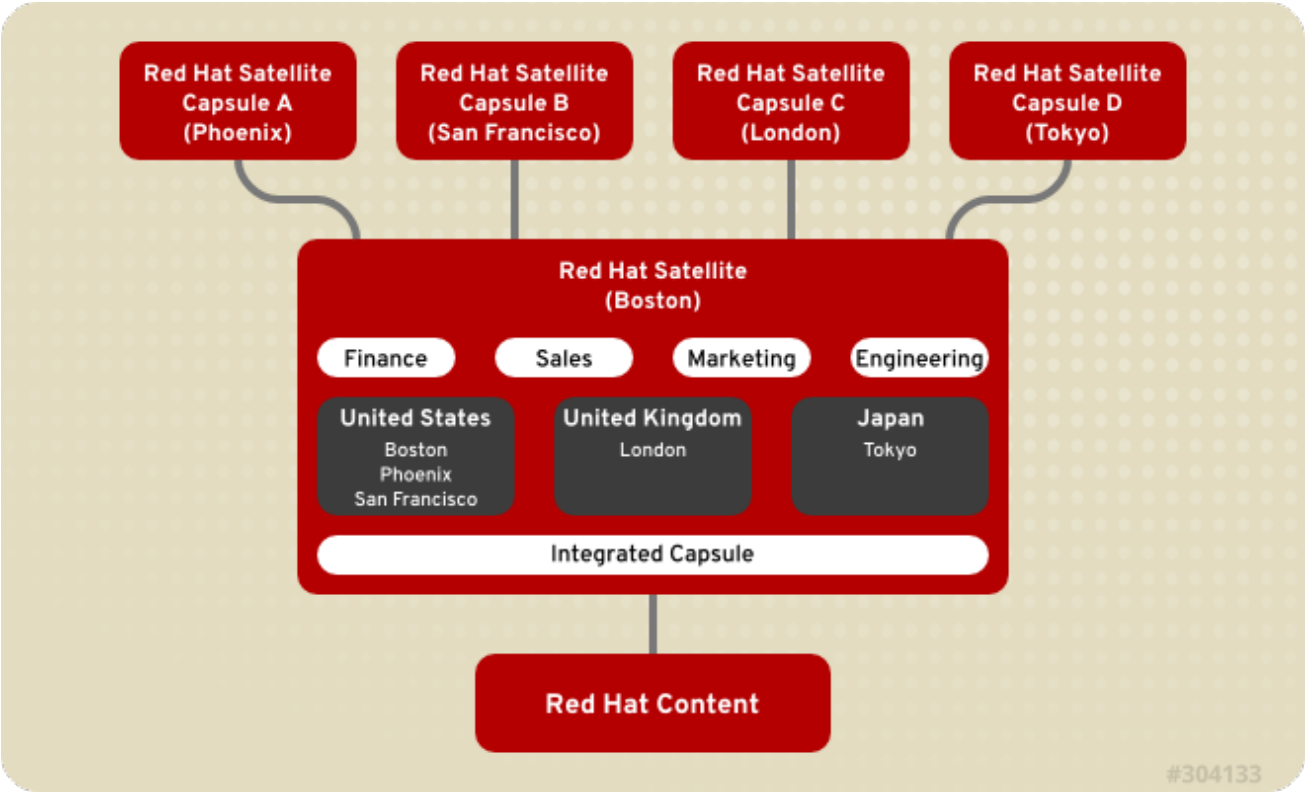


図3.1 Red Hat Satellite 6 のトポロジーサンプル

コンテンツと設定は主要な Satellite Server と特定のロケーションに割り当てられた Satellite Capsule Server 間で同期され、主要な Satellite Server が管理機能を保持します。

3.1. 組織

組織 は、ホストを所有権や目的、コンテンツ、セキュリティーレベルその他の区分に基づく論理グループに分類するために使用されます。

Web UI 内では、複数の組織を表示、作成、および管理することができます。ソフトウェアとホストのエンタイトルメントは多くの組織に割り振ることができ、それらの組織へのアクセスは制御することができます。

それぞれの組織は、1 つの Red Hat カスタマーアカウントにより作成され、使用される必要がありますが、それぞれのアカウントで複数の組織を管理することができます。サブスクリプションマニフェストは 1 つの組織にのみインポートでき、Satellite は別の組織にすでにアップロードされている証明書をアップロードしません。

Red Hat Satellite のインストールプロセスでは、**Default Organization (デフォルト組織)** という名前の組織が作成されます (別の名前が指定されない場合)。この組織名には対応するラベルがあります。

重要

新しいユーザーにデフォルトの組織が割り当てられていないと、そのユーザーのアクセスは制限されます。ユーザーにシステムの権限を付与するには、ユーザーをデフォルトの組織に割り当てた後に、そのユーザーでログアウトし、再度ログインします。

3.1.1. 組織の作成

以下の手順は、新規の組織を作成する方法を示しています。

手順3.1 組織の作成:

1. **Administer (管理) → Organizations (組織)** に移動します。
2. **New Organization (新規組織)** ボタンをクリックします。
3. **Name (名前)** フィールドに新規組織の名前を挿入します。
4. **Label (ラベル)** フィールドに新規組織のラベルを挿入します。
5. **Description (説明)** フィールドに新規組織の説明を挿入します。
6. **送信** をクリックします。
7. 新しい組織に割り当てるホストを選択します。
   - **Assign All (すべてを割り当て)** をクリックして組織のないすべてのホストを新しい組織に割り当てます。
   - **Manually Assign (手動割り当て)** をクリックして組織のないホストを手動で選択し、割り当てます。
   - **Proceed to Edit (編集に進む)** をクリックしてホストの割り当てを省略します。
8. Capsule Server、サブネット、コンピュートリソースなどの組織の設定詳細を指定します。「組織の編集」 で説明されているように、これらの設定はあとで変更できます。
9. **送信** をクリックします。

3.1.2. 組織のデバッグ証明書の作成

以下の手順は、組織のデバッグ証明書を生成し、ダウンロードする方法を示しています。デバッグ証明書は、組織のリポジトリーからすべてのコンテンツを参照することを可能にし、プロビジョニングテンプレートをエクスポートする際に必要になります。

手順3.2 新規組織デバッグ証明書の作成:

1. **Administer (管理) → Organizations (組織)** に移動します。
2. デバッグ証明書を生成する組織を選択します。
3. **Generate and Download (生成してダウンロード)** をクリックします。これにより、デバッグ証明書が生成されます。
4. 証明書ファイルを安全な場所に保存します。

注記

ダウンロードされるデバッグ証明書が組織内にまだ存在しない場合は、プロビジョニングテンプレートのダウンロード時に自動的に生成されます。

3.1.3. 組織のデバッグ証明書の使用

組織のリポジトリーコンテンツは、その組織のデバッグ証明書を持っている場合に、ブラウザーまたは API を使用して表示できます。前の項では、X.509 形式の証明書の作成およびダウンロードについて説明しています。ブラウザーを使用するには、最初に X.509 証明書をブラウザーがサポートする形式に変換し、次にその証明書をインポートする必要があります。**curl** ユーティリティーでは、別のファイルへの証明書およびキーの抽出のみを行います。

手順3.3 Firefox での組織のデバッグ証明書の使用:

1. 手順3.2「新規組織デバッグ証明書の作成:」 で説明されているように、組織の証明書を作成およびダウンロードします。
2. たとえば、デフォルトの組織の X.509 証明書を開きます。

```
$ vi 'Default Organization-key-cert.pem'
```

3. **-----BEGIN RSA PRIVATE KEY-----** から **-----END RSA PRIVATE KEY-----** までのファイルの内容を **key.pem** という名前のファイルにコピーします。
4. **-----BEGIN CERTIFICATE-----** から **-----END CERTIFICATE-----** までのいファイルの内容を **cert.pem** という名前のファイルにコピーします。
5. 以下のようにコマンドを入力して PKCS12 形式の証明書を作成し、パスワードまたはフレーズを入力します (要求された場合)。

```
$ openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -
export -in cert.pem -inkey key.pem -out organization_label.pfx -name
'organization_name'
Enter Export Password:
Verifying - Enter Export Password:
```

6. 設定タブを使用して、作成された **pfx** ファイルをブラウザーにインポートします。**Edit (編集) → Preferences (設定) → Advanced Tab (詳細タブ)** に移動します。**Certificates (証明書)** ビューの **View Certificates (証明書の表示)** を選択して **Certificate Manager (証明書マネージャー)** を開きます。**Your Certificates (ユーザーの証明書)** タブで、**Import (インポート)** をクリックし、ロードする **pfx** ファイルを選択します。証明書の作成時に、パスワードまたはフレーズを入力するよう求められます。
7. ブラウザーのアドレスバーに以下の形式の URL を入力してリポジトリーの参照を開始します。

```
http://satellite.example.com/pulp/repos/organization_label
```

Pulp は組織ラベルを使用するため、URL も組織ラベルを使用する必要があります。

手順3.4 curl での組織のデバッグ証明書の使用:

1. 手順3.2「新規組織デバッグ証明書の作成:」 で説明されているように、組織の証明書を作成およびダウンロードします。

2. たとえば、デフォルトの組織の X.509 証明書を開きます。

```
$ vi 'Default Organization-key-cert.pem'
```

3. **-----BEGIN RSA PRIVATE KEY-----** から **-----END RSA PRIVATE KEY-----** までのファイルの内容を **key.pem** という名前のファイルにコピーします。

4. **-----BEGIN CERTIFICATE-----** から **-----END CERTIFICATE-----** までのいファイルの内容を **cert.pem** という名前のファイルにコピーします。

5. リポジトリーの有効な URL を見つけます。前の手順で説明された参照方法を使用するか、Web UI を使用します。たとえば、Web UI を使用して、**Content (コンテンツ) → Products (製品)** に移動し、名前別に製品を選択します。**Repositories (リポジトリー)** タブで名前別にリポジトリーを選択し、**Published At (公開)** エントリーを探します。

6. **curl** を使用してリポジトリーにアクセスするには、以下のようにコマンドを使用します。

```
$ curl -k --cert cert.pem --key key.pem
http://satellite.example.com/pulp/repos/Default_Organization/Library
/content/dist/rhel/server/7/7Server/x86_64/sat-tools/6.2/os/
```

cert.pem と **key.pem** へのパスが適切な絶対パスであることを確認します。適切でないと、コマンドがサイレントで失敗します。

3.1.4. 組織の編集

手順3.5 組織の編集:

1. **Administer (管理) → Organizations (組織)** に移動します。

2. 編集する組織の名前をクリックします。

3. 左側の一覧から編集するリソースを選択します。

4. 必要な項目の名前をクリックし、それらを **選択された項目** の一覧に追加します。

5. **送信** をクリックします。

注記

管理者権限があるユーザーは、組織の編集時に **Users (ユーザー)** タブにリストされません。

3.1.5. 組織の削除

手順3.6 組織の削除:

組織は、ライフサイクル環境またはホストグループに関連付けられていない場合に削除できます。削除する組織にライフサイクル環境またはホストグループが関連付けられている場合は、**Organizations (組織)** に移動し、関連するタブをクリックしてそれらのライフサイクル環境またはホストグループを選択解除します。インストール中に作成されたデフォルトの組織は、Satellite 環境の関連付けされていないホストのプレースホルダーであるため、削除することは推奨されません。環境には常に少なくとも 1 つの組織が必要です。

1. **Administer (管理) → Organizations (組織)** に移動します。
2. 削除する組織の名前の右側にあるドロップダウンメニューから、**Delete (削除)** を選択します。
3. 警告ボックスが表示されます。

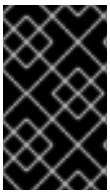
   ```
   Delete Organization?
   ```

4. **OK** をクリックして組織を削除します。

3.2. ロケーション

*ロケーション*は、地理的なロケーションに基づいて組織を論理グループに分割します。各ロケーションは 1 つの Red Hat カスタマーポータルアカウントにより作成および使用されますが、それぞれのアカウントで複数のロケーションと組織を管理できます。

Red Hat Satellite のインストールプロセスでは、**Default Location (デフォルトのロケーション)** という名前のロケーションが作成されます (別の名前が指定されない場合)。新しいユーザーにデフォルトのロケーションが割り当てられていないと、そのユーザーのアクセスは制限されます。ユーザーにシステムの権限を付与するには、デフォルトのロケーションを割り当て、そのユーザーでログアウトし、再度ログインします。



重要

デフォルトのロケーションは削除できませんが、必要に応じて名前を変更できます。Web UI またはコマンドラインを使用してデフォルトのロケーションを削除しようとすると、Satellite によりエラーメッセージが返されます。

3.2.1. ロケーションの作成

以下の手順は、ロケーションを作成する方法を示しています。

手順3.7 ロケーションの作成:

1. **Administer (管理) → Locations (ロケーション)** に移動します。
2. **New Location (新規ロケーション)** をクリックします。
3. **Name (名前)** フィールドに新規ロケーションの名前を挿入します。ネストされたロケーションを作成する場合は、ドロップダウンメニューから **Parent (親)** ロケーションを選択します。オプションで、ロケーションの **Description (説明)** を指定できます。**Submit (送信)** をクリックします。
4. 新規ロケーションに割り当てるホストを選択します。
   - **Assign All (すべてを割り当て)** をクリックしてロケーションのないすべてのホストを新しいロケーションに割り当てます。
   - **Manually Assign (手動割り当て)** をクリックしてロケーションのないホストを手動で選択し、割り当てます。
   - **Proceed to Edit (編集に進む)** をクリックしてホストの割り当てを省略します。

5. Capsule Server、サブネット、コンピュートリソースなどのロケーションの設定詳細を指定します。「ロケーションの編集」 で説明されているように、これらの設定はあとで変更できます。

6. **送信** をクリックします。

3.2.2. ロケーションの編集

手順3.8 ロケーションの編集:

1. **Administer (管理) → Locations (ロケーション)** に移動します。
2. 編集するロケーションの名前をクリックします。
3. 左側の一覧から編集するリソースを選択します。
4. 必要な項目の名前をクリックし、それらを **選択された項目** の一覧に追加します。
5. **送信** をクリックします。

3.2.3. ロケーションの削除

以下の手順は、既存のロケーションを削除する方法を示しています。現時点では、インストール中に作成されたデフォルトのロケーションの削除はサポートされていません。

手順3.9 ロケーションの削除:

1. **Administer (管理) → Locations (ロケーション)** に移動します。
2. 削除するロケーションの名前の右側にあるドロップダウンメニューから、**Delete (削除)** を選択します。

   警告ボックスが表示されます。

   ```
   Delete Location?
   ```

3. **OK** をクリックします。

3.3. ライフサイクル環境

アプリケーションライフサイクルは、アプリケーションライフサイクルの各ステージを表す *ライフサイクル環境*に分割されます。ライフサイクル環境はリンクされて *環境パス*を形成します。コンテンツは、必要に応じて環境パス上で次のライフサイクル環境にプロモートできます。たとえば、アプリケーションの特定のバージョンの開発が終了すると、このバージョンをテスト環境にプロモートし、次のバージョンの開発を開始することができます。

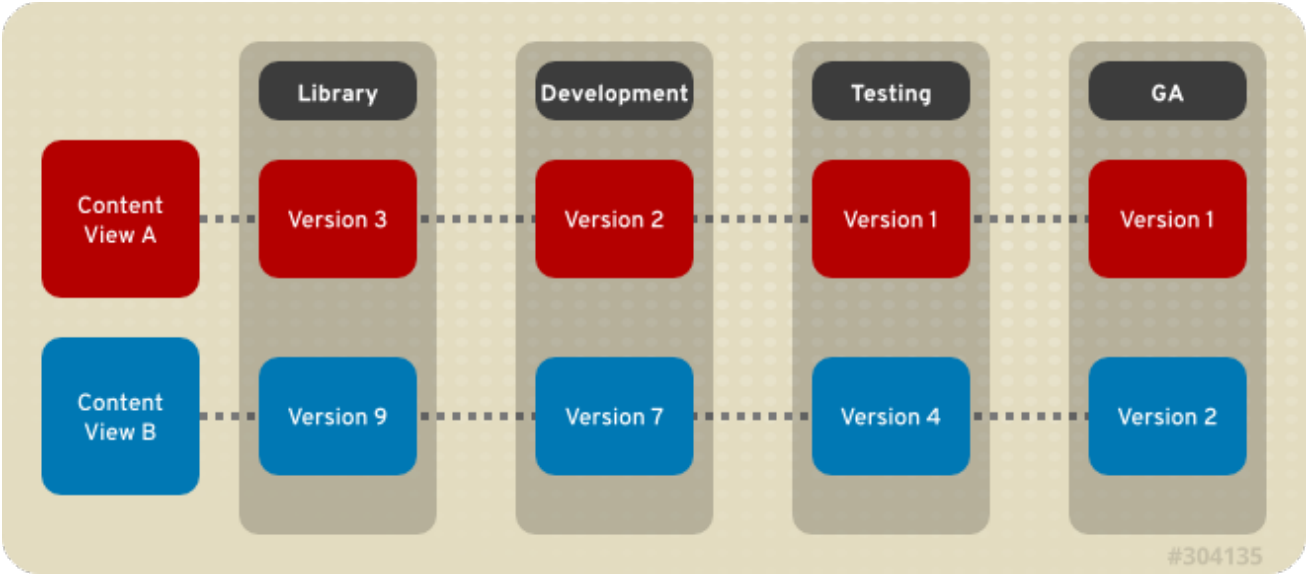


図3.2 4 つの環境を含む環境パス

3.3.1. ライフサイクル環境の作成

以下の手順では、Red Hat Satellite でライフサイクル環境を作成する方法を示します。

手順3.10 ライフサイクル環境の作成:

1. 左上隅にあるメニューから組織を選択します。
2. **Content (コンテンツ)** → **Life Cycle Environments (ライフサイクル環境)** をクリックしてから、**New Environment Path (新規環境パス)** をクリックします。
3. ライフサイクル環境の名前とラベルを挿入します (**Name (名前)** フィールドに自動的に入力されます)。**Description (説明)** フィールドはオプションです。
4. **Save (保存)** をクリックして環境を作成します。

3.3.2. コンテンツビューのプロモート

コンテンツビューと、2 つ以上のライフサイクル環境から構成される環境パスを作成したら、必要に応じてコンテンツビューをある環境から次の環境にプロモートできます。つまり、指定された環境に存在するコンテンツビューの最新バージョンがライフサイクル環境パスの次の環境にプロモート (つまり、コピー) されます。

コンテンツビューは、そのバージョンが存在しない環境にプロモートできます。ライフサイクル環境パスの次の環境が自動的に提示されますが、この値は上書きでき、必要に応じて別の環境にプロモートできます。

手順3.11 コンテンツビューのプロモート:

1. メインメニューで **Content (コンテンツ)** → **Content Views (コンテンツビュー)** をクリックします。
2. **Name (名前)** 列で、プロモートするコンテンツビューの名前をクリックします。
3. **Versions (バージョン)** タブで、最新バージョンを特定し、**Promote (プロモート)** をクリックします。

4. コンテンツビューをプロモートするプロモーションパスを特定し、適切なライフサイクル環境を選択して、**Promote Version (バージョンのプロモート)** をクリックします。

5. プロモーションが完了したら、**Versions (バージョン)** タブが更新されコンテンツビューの新しいステータスが表示されます。

3.3.3. Satellite Server からのライフサイクル環境の削除

以下の手順では、Red Hat Satellite からライフサイクル環境を削除する方法を示します。

手順3.12 ライフサイクル環境の削除:

1. メインメニューで **Content (コンテンツ) → Life Cycle Environments (ライフサイクル環境)** をクリックします。

2. 削除するライフサイクル環境の名前をクリックし、**Remove Environment (環境の削除)** をクリックします。

3. 確認ダイアログボックスで **Remove (削除)** をクリックして環境を削除します。

注記

環境パスの最新の環境のみを削除できます。たとえば、3 つの環境が **Library**、**Dev**、および **Prod** の順序で存在する場合は、**Dev** を削除する前に **Prod** を削除する必要があります。**Library** 環境は削除できません。

3.3.4. Capsule Server からのライフサイクル環境の削除

ライフサイクル環境を Capsule Server から削除する理由は複数あります。以下のような理由があります。

- ライフサイクル環境とホストシステムとの関連性がなくなった場合
- ライフサイクル環境が Capsule Server に誤って追加された場合

手順3.13 Capsule Server からのライフサイクル環境の削除:

1. root ユーザーとして Satellite Server CLI にログインします。

2. 一覧から必要な Capsule Server を選択し、その **ID** をメモします。

```
# hammer capsule list
```

Capsule Server の詳細は、以下のコマンドを使って検証することができます。

```
# hammer capsule info --id capsule_id_number
```

3. Capsule Server に現在割り当てられているライフサイクル環境の一覧を検証し、**environment id** をメモします。

```
# hammer capsule content lifecycle-environments --id
capsule_id_number
```

4. Capsule Server からのライフサイクル環境を削除します。

```
# hammer capsule content remove-lifecycle-environment --id
capsule_id_number --environment-id environment_id
```

ここで、

- *capsule_id_number* は Capsule Server の ID 番号です。
- *environment_id* は、ライフサイクル環境の ID 番号です。

Capsule Server から削除するすべてのライフサイクル環境に対してこの手順を繰り返します。

5. Satellite Server の環境にあるコンテンツを Capsule Server に同期します。

```
# hammer capsule content synchronize --id capsule_id_number
```

3.4. インポート履歴の表示

以下の手順は、Red Hat Satellite でインポート履歴を表示する方法を示しています。

手順3.14 インポート履歴の表示:

1. **コンテンツ → Red Hat サブスクリプション** をクリックします。
2. **マニフェストの管理** ボタンをクリックします。
3. **インポートの履歴** タブをクリックします。

第4章 ユーザーとロール

*ユーザー*では、システムを使用する各個人の一連の詳細情報を定義します。ユーザーにはデフォルトの組織と環境を割り当て、新しいエンティティーを作成する際にこれらのデフォルト値を自動的に使用することができます。また、ユーザーには 1 つ以上の**ロール**を割り当てることもできます。これにより、ユーザーには組織と環境を参照および管理する権限が与えられます。ユーザーの使用の詳細については、「ユーザーの作成および管理」 を参照してください。

複数のユーザーのパーミッションは、*ユーザーグループ*を使用することにより一括して管理できます。また、ユーザーグループ自体をさらにグループ化してパーミッションの階層を作成できます。ユーザーグループの作成の詳細については、「ユーザーグループの作成」 を参照してください。

*ロール*では、一連のパーミッションおよびアクセスレベルを定義します。各ロールには、ロールに許可された*アクション*を指定する 1 つ以上の*パーミッションフィルター*が含まれます。アクションは、*リソースタイプ*に従ってグループ化されます。ロールが作成されたら、そのロールにはユーザーとユーザーグループを関連付けることができます。この場合は、ユーザーの大きなグループに同じ一連のパーミッションセットを割り当てることができます。Red Hat Satellite では、事前定義された一連のロールが提供され、「ロールの作成および管理」 で説明されているようにカスタムロールおよびパーミッションフィルターを作成することもできます。

4.1. ユーザーの作成および管理

Red Hat Satellite では、管理者はユーザーを作成、変更、および削除できます。また、ロールをユーザーに割り当てることによってアクセスパーミッションを設定することもできます。

4.1.1. ユーザーの作成

以下の手順は、ユーザーを作成する方法を示しています。

手順4.1 ユーザーの作成:

1. **Administer (管理) → Users (ユーザー)** をクリックしてから、**New User (新規ユーザー)** をクリックします。
2. **User (ユーザー)** タブで、必要な詳細を入力します。
3. **ロケーション** タブで、このユーザーに必要なロケーションを選択します。
4. **Organizations (組織)** タブで、このユーザーがアクセスできる組織を選択します。デフォルトでは、現在アクティブな組織が選択されます。複数の組織を指定する場合は、ドロップダウンリストからユーザーログインのデフォルト組織を選択できます。
5. **ロール** タブで、このユーザーに必要なロールを選択します。アクティブなロールが右側のパネルに表示されます。
6. **送信** をクリックしてユーザーを作成します。

4.1.2. ユーザーの編集

以下の手順は、既存ユーザーの詳細を編集する方法を示しています。

手順4.2 既存ユーザーの編集:

1. **Administer (管理) → Users (ユーザー)** に移動します。

2. 変更するユーザーのユーザー名をクリックします。ユーザーに関する全般情報が右側に表示されます。

3. **User (ユーザー)** タブで、ユーザーのユーザー名、名、姓、電子メールアドレス、デフォルトロケーション、デフォルト組織、言語、およびパスワードを変更できます。

4. **Locations (ロケーション)** タブで、割り当てられたユーザーのロケーションを変更できます。

5. **Organizations (組織)** タブで、割り当てられたユーザーの組織を変更できます。

6. **Roles (ロール)** タブで、割り当てられたユーザーのロールを変更できます。

7. **Save （保存）** をクリックして、変更を保存します。

4.1.3. ユーザーへのロールの割り当て

デフォルトでは、新しいユーザーにはロールが割り当てられません。以下の手順は、ユーザーに 1 つ以上のロールを割り当てる方法を示しています。事前定義されたロールから選択するか、「ロールの作成」 で説明されているようにカスタムロールを定義できます。同様の手順はユーザーグループに適用できます。

手順4.3 ユーザーへのロールの割り当て:

1. **Administer (管理) → Users (ユーザー)** をクリックします。作成されたユーザーアカウントがリストされない場合は、現在適切な組織を表示していることを確認します。Satellite ですべてのユーザーをリストするには、**Default Organization （デフォルト組織）**、次に **Any Organization （任意の組織）** をクリックします。組織ビューは **Any Context （任意のコンテキスト）** に変更されます。

2. 変更するユーザーのユーザー名をクリックします。ユーザーに関する全般情報が右側に表示されます。

3. **Locations (ロケーション)** タブをクリックし、何も割り当てられていない場合はロケーションを選択します。

4. **Organizations (組織)** タブをクリックし、組織が割り当てられていることを確認します。

5. **Roles (ロール)** タブをクリックして利用可能な割り当て済みロールのリストを表示します。

6. **Roles （ロール）** リストで、ユーザーに割り当てるロールを選択します。リストには、事前定義されたロールとカスタムロールが含まれます (表4.1「Red Hat Satellite で利用可能な事前定義済みロール」 を参照)。または、**Administrator （管理者）** チェックボックスを選択して、選択されたユーザーに利用可能なすべてのパーミッションを割り当てます。

7. **保存** をクリックします。

ユーザーに割り当てられたロールを参照するには、**Roles (ロール)** タブをクリックします。割り当てられたロールは、**Selected items （選択したアイテム）** 下にリストされます。ロールを削除するには、**Selected items （選択したアイテム）** でロール名をクリックします。この結果、ロールが削除されます。

4.1.4. 電子メール通知の設定

電子メール通知は、ユーザーごとに設定し、デフォルトでは有効になりません。電子メール通知を個人の電子メールアドレスではなくグループの電子メールアドレスに送信する場合は、グループの電子メー

ルアドレスと最小の Satellite パーミッションでユーザーアカウントを作成し、そのユーザーアカウントを必要な通知タイプにサブスクライブします。

送信 Satellite 電子メールの設定に関する一般情報については、Red Hat Satellite Installation Guide を参照してください。

注記

電子メール通知を受信するには、ユーザーアカウントに有効な電子メールアドレスが含まれる必要があります。ユーザーアカウントに関連付けられた電子メールアドレスを確認するには、**Administer (管理) → Users (ユーザー)**に移動し、**Email address (電子メールアドレス)** フィールドを確認します。

手順4.4 電子メール通知の設定:

1. **Administer (管理) → Users (ユーザー)** に移動します。
2. 編集するユーザーの **Username (ユーザー名)** をクリックします。
3. **Email Preferences (電子メール設定)** タブをクリックし、**Mail enabled (メールの有効化)** を選択して電子メール通知を有効にします。
4. ユーザーが受信する通知を選択します。
   - **Audit summary (監査の概要)** は、Satellite Server で監査されたすべてのアクティビティーの概要です。これらの通知を有効にするには、ドロップダウンリストから電子メールの頻度 (**Daily (毎日)**、**Weekly (毎週)**、または **Monthly (毎月)**) を選択します。関連するクエリーフィールドにクエリーを入力して、含まれる監査アクティビティーを絞り込みます。
   - **Host built (ホストの構築)** は、ホストが構築されたときに送信される通知です。これらの通知を有効にするには、ドロップダウンメニューから **Subscribe (サブスクライブ)** を選択します。
   - **Host errata advisory (ホストエラータアドバイザリー)** は、ユーザーが管理するホストの適用およびインストール可能なエラータの概要です。これらの通知を有効にするには、ドロップダウンリストから電子メールの頻度 (**Daily (毎日)**、**Weekly (毎週)**、または **Monthly (毎月)**) を選択します。
   - **OpenSCAP policy summary (OpenSCAP ポリシー概要)** は、OpenSCAP ポリシーレポートとその結果の概要です。これらの通知を有効にするには、ドロップダウンリストから電子メールの頻度 (**Daily (毎日)**、**Weekly (毎週)**、または **Monthly (毎月)**) を選択します。
   - **Promote errata (エラータのプロモート)** は、コンテンツビューのプロモーション後にのみ送信される通知です。これには、プロモートされたコンテンツビューに登録された適用およびインストール可能なエラータの概要が含まれます。この場合は、どのアップデートがどのホストに適用されたかを監視できます。これらの通知を有効にするには、ドロップダウンメニューから **Subscribe (サブスクライブ)** を選択します。
   - **Puppet error state (Puppet エラー状態)** は、ホストが Puppet に関連するエラーを報告したあとに送信される通知です。これらの通知を有効にするには、ドロップダウンメニューから **Subscribe (サブスクライブ)** を選択します。

- **Puppet summary (Puppet 概要)** は、Puppet レポートの概要です。これらの通知を有効にするには、ドロップダウンリストから電子メールの頻度 (**Daily (毎日)**、**Weekly (毎週)**、または **Monthly (毎月)**) を選択します。

- **Sync errata (エラータの同期)** は、リポジトリーの同期後にのみ送信される通知です。これには、同期で導入された新しいエラータの概要が含まれます。これらの通知を有効にするには、ドロップダウンメニューから **Subscribe (サブスクライブ)** を選択します。

5. **送信** をクリックします。

電子メール配信のテスト

ユーザーアカウントに関連付けられた電子メールアドレスへの電子メール配信をテストするには、Satellite Web UI を開き、**Administer (管理) → Users (ユーザー)** に移動し、ユーザー名をクリックし、**Email Preferences (電子メール設定)** タブをクリックして、**Test email (電子メールのテスト)** をクリックします。ユーザーの電子メールアドレスにテスト電子メールメッセージがすぐに送信されます。メッセージが受信されない場合は、最初にユーザーの電子メールアドレスを確認し、次に Satellite Server の電子メール設定を確認します。この後で、ファイアウォールとメールサーバーのログを調べる必要があることがあります。

4.1.5. ユーザーの削除

以下の手順は、既存のユーザーを削除する方法を示しています。

手順4.5 ユーザーの削除:

1. メインメニューで **Administer (管理) → Users (ユーザー)** をクリックして **Users (ユーザー)** ページを表示します。

2. 削除するユーザー名の右側にある **Delete (削除)** リンクをクリックします。

3. 警告ボックスで、**OK** をクリックしてユーザーを削除します。

4.2. ユーザーグループの作成

Red Hat Satellite では。ユーザーのグループにパーミッションを割り当てることができます。また、ユーザーグループを他のユーザーグループのコレクションとして作成することもできます。外部認証ソースを使用している場合は、「外部ユーザーグループの設定」 で説明されているように Satellite ユーザーグループを外部ユーザーグループに対してマップできます。

ユーザーグループは組織コンテキストで定義されます。したがって、ユーザーグループにアクセスする前に組織を選択する必要があります。

手順4.6 ユーザーグループの作成:

1. **Administer (管理) → User Groups (ユーザーグループ)** に移動して、Satellite のユーザーグループを表示します。

2. **New User Group (新規ユーザーグループ)** をクリックます。

3. **User group (ユーザーグループ)** タブで、新規ユーザーグループの名前を指定し、ユーザーのリストからグループメンバーを選択します。以前に作成されたユーザーグループを含めるには、追加するグループの名前の横にあるチェックボックスを選択します。

4. **Roles（ロール）**タブで、ユーザーグループに割り当てるロールを選択します。または、**Administrator（管理者）**チェックボックスを選択して利用可能なすべてのパーミッションを割り当てます。

5. **Submit（送信）**をクリックしてユーザーグループを作成します。

4.3. ロールの作成および管理

Red Hat Satellite では、標準的なタスクに十分なパーミッションを持つ一連の事前定義済みロールが提供されます (表4.1「Red Hat Satellite で利用可能な事前定義済みロール」 を参照)。また、カスタムロールを設定し、1 つ以上のパーミッションフィルターをそれらに割り当てることもできます。パーミッションフィルターでは、特定のリソースタイプに許可されるアクションを定義します。特定の Satellite プラグインによりロールが自動的に作成されます。

表4.1 Red Hat Satellite で利用可能な事前定義済みロール

Role (ロール)	ロールで提供されるパーミッション[a]
Anonymous	他のロールに関係なく、各ユーザーに与えられる一連のパーミッション。
Discovery manager	検出されたホストを表示、プロビジョニング、編集、および破棄し、検出ルールを管理します。
Discovery reader	ホストと検出ルールを表示します。
Boot disk access	起動ディスクをダウンロードします。
Red Hat Access Logs	ログビューアーとログを表示します。
マネージャ	最も広範なパーミッションセット。各リソースタイプからのほとんどのアクションが有効になります。
Edit partition tables	パーティションテーブルを表示、作成、編集、および破棄します。
View hosts	ホストを表示します。
Edit hosts	ホストを表示、作成、編集、破棄、および構築します。
Viewer	Satellite 構造、ログ、および統計の各要素の設定を表示できる機能を提供する受動的なロール。
Site manager	Manager ロールの制限バージョン。
Tasks manager	Satellite タスクを表示および編集します。
Tasks reader	Satellite タスクを表示します。

Role (ロール)	ロールで提供されるパーミッション[a]

[a] 事前定義されたロールに関連付けられた一連の許可済みアクションは、「ロールのパーミッションの表示」 で説明されているように特権ユーザーが参照できます。

4.3.1. ロールの作成

以下の手順は、ロールを作成する方法を示しています。

手順4.7 ロールの作成:

1. **Administer (管理) → Roles (ロール)** に移動します。
2. **New Role** をクリックします。
3. ロールの **名前** を入力します。
4. **Submit (送信)** をクリックして新規ロールを保存します。

目的を達成するために、ロールにはパーミッションが含まれる必要があります。ロールの作成後は、「ロールへのパーミッションの追加」 に進んでください。

注記

既存のロールをクローンすると、ロール作成の時間を節約できます (特に、既存のパーミッションセットに基づく新しいロールを作成する場合)。ロールをクローンするには、**Administer (管理) → Roles (ロール)** に移動し、コピーするロールの右側にあるドロップダウンリストから **Clone (クローン)** を選択します。新しいロールの名前を選択し、必要に応じてパーミッションを変更します。

4.3.2. ロールへのパーミッションの追加

以下の手順はパーミッションをロールに追加する方法を示しています。

手順4.8 ロールへのパーミッションの追加:

1. **Administer (管理) → Roles (ロール)** に移動します。
2. 必要なロールの右側にあるドロップダウンリストから **Add Filter (フィルターの追加)** を選択します。
3. ドロップダウンリストから **Resource type (リソースタイプ)** を選択します。**(Miscellaneous)** グループには、どのリソースグループにも関連付けられていないパーミッションが含まれます。
4. 選択するパーミションを **Permission (パーミッション)** リストでクリックします。
5. パーミッションを **Unlimited (無制限)** にするかどうかを選択します。このオプションはデフォルトで選択されるため、パーミションは選択されたタイプのすべてのリソースに適用されます。**Unlimited (無制限)** チェックボックスを無効にすると、**Search (検索)** フィールドがアクティベートされます。このフィールドでは、Red Hat Satellite 6 の検索構文を使用して詳細なフィルタリングを指定できます。詳細については、「詳細なパーミッションフィルタリング」 を参照してください。

6. **Next (次へ)** をクリックします。

7. **送信 (Submit)** をクリックして変更を保存します。

4.3.3. ロールのパーミションの表示

以下の手順は、既存のロールに割り当てられたパーミションを表示する方法を示しています。

手順4.9 ロールに関連付けられたパーミッションの表示:

1. **Administer (管理) → Roles (ロール)** に移動します。

2. 必要なロールの右側にある **Filters (フィルター)** をクリックして **Filters (フィルター)** ページに移動します。

Filters (フィルター) ページには、リソースタイプ別にグループ化されたロールに割り当てられたパーミッションの表が含まれます。また、このページでは、Satellite システムで使用できるパーミッションとアクションの完全な表を生成できます。手順については、手順4.10「パーミッションの完全な表の作成:」 を参照してください。

手順4.10 パーミッションの完全な表の作成:

1. 必要なパッケージがインストールされていることを確認します。Satellite Server で以下のコマンドを実行します。

```
# yum install tfm-rubygem-foreman*
```

2. 以下のコマンドで Satellite コンソールを起動します。

```
# foreman-rake console
```

コンソールに以下のコードを挿入します。

```
f = File.open('/tmp/table.html', 'w')

result = Foreman::AccessControl.permissions.sort {|a,b|
a.security_block <=> b.security_block}.collect do |p|
      actions = p.actions.collect { |a| "<li>#{a}</li>" }
      "<tr><td>#{p.name}</td><td><ul>#{actions.join('')}</ul></td>
<td>#{p.resource_type}</td></tr>"
end.join("\n")

f.write(result)
```

上記の構文により、パーミッションの表が作成され、**/tmp/table.html** ファイルに保存されます。

3. **Ctrl+D** を押して、Satellite コンソールを終了します。**/tmp/table.html** の最初の行に以下のテキストを挿入します。

```
<table border="1"><tr><td>Permission name</td><td>Actions</td>
<td>Resource type</td></tr>
```

/tmp/table.html の最後の以下のテキストを追加します。

```
</table>
```

4. Web ブラウザーで **/tmp/table.html** を開いて、表を参照します。

4.3.4. ロールの削除

以下の手順は、既存のロールを削除する方法を示しています。

手順4.11 ロールの削除:

1. **Administer (管理) → Roles (ロール)** に移動します。
2. 削除するロールの右側にあるドロップダウンリストから **Delete (削除)** を選択します。
3. 表示された警告ボックスで、**OK** をクリックしてロールを削除します。

4.4. 詳細なパーミッションフィルタリング

「ロールへのパーミッションの追加」 で説明されているように、Red Hat Satellite では、リソースタイプの選択済みインスタンスに対する設定済みユーザーパーミッションを制限できます。これらの詳細なフィルターは Satellite データベースに対するクリリーであり、ほとんどのリソースタイプでサポートされています。

詳細なフィルターを作成するには、**Edit Filter（フィルターの編集）**ページの **Search（検索）**フィールドにクエリーを指定します。アクティブにするフィールドに対して **Unlimited（無制限）**チェックボックスを選択解除します。クエリーの形式は以下のようになります。

```
field_name operator value
```

ここで、

- *field_name* は、問い合わせるフィールドを示します。利用可能なフィールド名の範囲はリソースタイプによって異なります。たとえば、**Partition Table** リソースタイプでは、クエリーパラメーターとして **family**、**layout**。および **name** が提供されます。
- *operator* は、*field_name* と *value* との間の比較タイプを指定します。適用可能な演算子の概要については、表4.2「詳細な検索に対してサポートされる演算子」 を参照してください。
- *value* は、フィルタリングに使用される値です。この値は、組織の名前などです。2 つの種類のワイルドカード文字がサポートされ、アンダースコア (_) は単一の文字を置換し、パーセント記号 (%) はゼロ以上の文字を置換します。

ほとんどのリソースタイプに対して、**Search（検索）**フィールドは利用可能なパラメーターを示すドロップダウンリストを提供します。このリストは、検索フィールドにカーソルを置くと表示されます。多くのリソースタイプに対しては、**and** 演算子と **or** 演算子を使用してクエリーを組み合わせることもできます。

表4.2 詳細な検索に対してサポートされる演算子

オペレーター	説明
=	**Is equal to**。テキストフィールド向けの、大文字と小文字を区別する等価比較。

オペレーター	説明
!=	**Is not equal to**。= 演算子の反転。
~	**Like**。テキストフィールド向けの、大文字と小文字を区別する頻出検索。
!~	**Not like**。~ 演算子の反転。
^	**In**。特定の文字列を含む、テキストフィールド向けの、大文字と小文字を区別する検索。
!^	**Not in**。^ 演算子の反転。
>, >=	**Greater than**、**greater than or equal to**。数値フィールドに対してのみサポートされます。
<, <=	**Less than**、**less than or equal to**。数値フィールドに対してのみサポートされます。

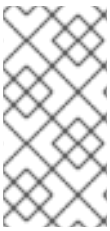
たとえば、以下のクエリーは、host-editors という名前のグループのホストに対してのみ、ホストのリソースタイプに指定されたパーミッションを適用します。

```
hostgroup = host-editors
```

また、選択された環境に対するパーミッションを制限することもできます。これを行うには、**Search (検索)** フィールドに環境名を指定します。以下に例を示します。

```
Dev
```

管理者として、選択されたユーザーが環境パスの特定の部分を変更することを許可できます。上記のフィルターを使用すると、アプリケーションライフサイクルの開発段階にあるコンテンツを使用して作業できますが、そのコンテンツは本番稼働されるとアクセスできなくなります。



注記

Satellite では、検索条件はアクションを作成するために適用されません。たとえば、検索フィールドで **create_locations** アクションを **name = "Default Location"** 式で制限しても、新しく作成されたロケーションにユーザーがカスタム名を割り当てることを防ぐことはできません。

パーミッションフィルターを使用して、特定の組織またはロケーションにユーザーパーミッションを制限できます。ただし、リソースタイプにより、**Locations (ロケーション)** タブと **Organizations (組織)** タブという形で GUI が提供されます。これらのタブでは、利用可能な組織とロケーションのリストから選択できます。例4.1「組織に固有なマネージャーロールの作成」 を参照してください。

例4.1 組織に固有なマネージャーロールの作成

この例では、**org-1** という名前の単一の組織に制限されたマネージャーロールを作成する方法を示します。

1. **Administer (管理) → Roles (ロール)** に移動します。

2. 既存の **Manager (マネージャー)** ロールをクローンします。**Filters （フィルター）** ボタンの横にあるドロップダウンリストから **Clone (クローン)** を選択します。この結果、クローンされたロールの名前 (たとえば、**org-1 Manager**) を挿入するよう求められます。

3. **org-1 Manager** の横にある **Filters （フィルター）** をクリックして、ロールに関連付けられたフィルターを表示します。すべてのフィルターは無制限と示されます。

4. 各フィルターに対して、**Edit （編集）** をクリックします。

5. フィルターに **Organizations （組織）** タブが含まれる場合は、そのタブに移動します。含まれない場合は、制限できないグローバル設定です。

6. **Organizations （組織）** タブで、**org-1** を選択します。**Submit （送信）** をクリックします。

7. 制限されたフィルターは、無制限と示されなくなります。この時点で、**org-1 Manager** ロールを割り当てられたユーザーは選択された組織の管理タスクのみ実行できます。

第5章 バックアップおよび災害復旧

本章では、災害発生時に Red Hat Satellite デプロイメントと関連データを維持するために必要な最小限および一般的なバックアップ手順と復元手順につい説明します。デプロイメントでカスタム設定をする場合は、バックアップおよび災害復旧ポリシーを計画するときにこれらの手順を考慮する必要があります。

5.1. RED HAT SATELLITE SERVER のバックアップ

本項では、Satellite Server とすべての関連データの完全なバックアップを作成するのに必要なプロセスについて説明します。異なる場所にバックアップすることが推奨されます。また、別のシステムの別のストレージデバイスにバックアップすることが強く推奨されます。バックアップ中は Satellite サービスが利用できないため、バックアップは稼働率が低い時間にスケジュールできます (たとえば、**cron** を使用)。

注記

スケジュールされたバックアップを計画するときは、同じ時間に他のタスクが他の管理者によってスケジュールされないようにしてください。これは、管理者が異なる場所とタイムゾーンで働いている場合に特に重要です。

Red Hat Satellite 6.2 では、Pulp コンテンツを除く増分バックアップと中間バックアップを実行する **katello-backup** スクリプトにオプションが追加されます。使用方法を参照するには、以下のコマンドを入力します。

```
# katello-backup --help
```

katello-backup スクリプトを実行すると、指定したバックアップディレクトリーのタイムスタンプサブディレクトリーにデータが格納されます。**katello-backup** スクリプトによりバックアップは上書きされず、バックアップまたは増分バックアップから復元するときに適切なサブディレクトリーを選択する必要があります。**katello-backup --online-backup** は現在サポートされていないため、使用しないでください。

手順5.1 Red Hat Satellite Server のバックアップ:

1. この手順では、完全なオフラインバックアップを実行します。バックアップの場所に、以下のすべてのディレクトリーのコピーを保存するのに十分なディスク領域があることを確認します。
   - **/etc/**
   - **/var/lib/pulp/**
   - **/var/lib/mongodb/**
   - **/var/lib/pgsql/**

   この領域は非常に大きいため、適切に計画してください。
2. 他の Satellite Server ユーザーに、すべての変更を保存するよう要求し、バックアップ中に Satellite サービスが利用できないことを警告します。同じ時間に他のタスクがバックアップとしてスケジュールされていないことを確認します。
3. バックアップスクリプトを実行します。

```
# katello-backup backup_directory
```

katello-backup スクリプトを実行すると、バックアップに影響を与える可能性があるすべてのサービスが停止し、バックアップが実行され、必要なサービスが再起動されます。バックアップファイルを作成するときにターゲットディレクトリーが存在しない場合、そのディレクトリーはスクリプト によって作成されます。

コピーするデータのサイズが原因で、このプロセスが完了するには長い時間がかかることがあります。

手順5.2 Pulp コンテンツなしでのバックアップの実行:

この手順では、オフラインバックアップが実行されますが、Pulp ディレクトリーの内容は除外されます。このバックアップは、デバッグに役に立ち、Pulp データベースのバックアップに時間を費やさずに設定ファイルへのアクセスを提供することを目的としています。Pulp コンテンツを含まないディレクトリーから復元することはできません。

バックアップの場所に、以下のすべてのディレクトリーのコピーを保存するのに十分なディスク領域があることを確認します。

- **/etc/**
- **/var/lib/mongodb/**
- **/var/lib/pgsql/**

1. 他の Satellite Server ユーザーに、すべての変更を保存するよう要求し、バックアップ中に Satellite サービスが利用できないことを警告します。同じ時間に他のタスクがバックアップとしてスケジュールされていないことを確認します。
2. バックアップスクリプトを実行します。

```
# katello-backup --skip-pulp-content backup_directory
```

katello-backup スクリプトを実行すると、バックアップに影響を与える可能性があるすべてのサービスが停止し、バックアップが実行され、必要なサービスが再起動されます。

手順5.3 増分バックアップの実行:

この手順では、前回のバックアップ以降のすべての変更のオフラインバックアップを実行します。完全バックアップを土台として使用して最初の増分バックアップを実行します。以下のディレクトリーのすべての変更のコピーを保存するのに十分なディスク領域があることを確認します。

- **/etc/**
- **/var/lib/pulp/**
- **/var/lib/mongodb/**
- **/var/lib/pgsql/**

1. 他の Satellite Server ユーザーに、すべての変更を保存するよう要求し、バックアップ中に Satellite サービスが利用できないことを警告します。同じ時間に他のタスクがバックアップとしてスケジュールされていないことを確認します。
2. バックアップスクリプトを実行します。

Pulp コンテンツがある場合:

```
# katello-backup new_backup_directory --incremental
previous_backup_directory
```

Pulp コンテンツがない場合:

```
# katello-backup new_backup_directory --skip-pulp-content --
incremental previous_backup_directory
```

katello-backup スクリプトを実行すると、バックアップに影響を与える可能性があるすべてのサービスが停止し、バックアップが実行され、必要なサービスが再起動されます。前回のバックアップよりも古いバックアップを土台として使用し、対応する増加分を使用して増分バックアップを実行できます。少なくとも問題がない最後の完全バックアップと復元する増分バックアップの完全なシーケンスを保持します。

5.2. バックアップからの RED HAT SATELLITE SERVER の復元

本項では、「Red Hat Satellite Server のバックアップ」の手順の結果として作成されたバックアップデータから Red Hat Satellite Server を完全に復元する方法について説明します。このプロセスでは、バックアップが生成されたのと同じサーバーでバックアップが復元されます。元のシステムが利用できない場合は、同じ設定で同じ構成をプロビジョニングします (特に、ホスト名は同じである必要があります)。

重要

以下にプロセスでは、完全な Red Hat Satellite の復元について説明します。このプロセスでは、ターゲット Satellite インスタンスからすべてのデータが削除されます。以下の条件を満たすようにしてください。

- 適切なインスタンスに対して復元を行います。Red Hat Satellite インスタンスの設定、 パッケージバージョン、 およびエラータは元のシステムと同じである必要があります。
- すべてのコマンドは、アーカイブがバックアップ中に作成されたディレクトリー内で **root** として実行されます。
- すべての SELinux コンテキストが適切です。以下のコマンドを実行して適切な SELinux コンテンツを復元します。

  ```
  # restorecon -Rnv /
  ```

手順5.4 完全バックアップからの Red Hat Satellite の復元方法:

1. 『Red Hat Satellite 6 Installation Guide』[1] の手順に従って Satellite 6 をインストールします。
2. バックアップデータを Satellite のローカルファイルシステム (**/var/tmp/satellite-backup/** など) にコピーします。Satellite Server でこのデータを格納するのに十分な領域と、復元後にバックアップ内に含まれる **/etc/** ディレクトリーと **/var/** ディレクトリー内のすべてのデータを格納するのに十分な領域があることを確認します。
3. 復元スクリプトを実行します。

   -

```
# katello-restore backup_directory
```

ここで、*backup_directory* は、バックアップデータを含むディレクトリーです。ターゲットディレクトリーは設定ファイルから読み取られます。復元の試行時にターゲットディレクトリーが存在しない場合は、エラーが発生し、適切なディレクトリーを指定するよう求められます。コピーするデータのサイズが原因で、このプロセスが完了するのに長い時間がかかることがあります。増分バックアップが存在する場合は、手順5.5「増分バックアップからの Red Hat Satellite の復元方法:」 を参照してください。

このプロセスが完了したら、すべてのサービスが実行され、Satellite Server を使用できるはずです。

手順5.5 増分バックアップからの Red Hat Satellite の復元方法:

1. 『Red Hat Satellite 6 Installation Guide』[2] の手順に従って Satellite 6 をインストールします。
2. 手順5.4「完全バックアップからの Red Hat Satellite の復元方法:」で説明されたように最後の完全バックアップを復元します。
3. バックアップデータを Satellite のローカルファイルシステム (**/var/tmp/satellite-backup/** など) にコピーします。Satellite Server でこのデータを格納するのに十分な領域と、復元後にバックアップ内に含まれる **/etc/** ディレクトリーと **/var/** ディレクトリー内のすべてのデータを格納するのに十分な領域があることを確認します。
4. 復元スクリプトを実行します。

```
# katello-restore backup_directory_X
```

ここで、*backup_directory_X* は増分バックアップが含まれるディレクトリーです。作成されたのと同じ順序で増分バックアップを復元します (たとえば、*backup_directory_1*、*backup_directory_2*)。

このプロセスが完了したら、すべてのサービスが実行され、Satellite Server を使用できるはずです。

---

[1] https://access.redhat.com/documentation/en/red-hat-satellite/6.2/single/installation-guide/

[2] https://access.redhat.com/documentation/en/red-hat-satellite/6.2/single/installation-guide/

第6章 RED HAT SATELLITE SERVER の管理

本章では、関連するログファイルに関する情報、デバッグロギングを有効にする方法、サポートケースを開き、関連するログ tar ファイルを添付する方法、Red Hat Insight を使用してシステムを積極的に診断する方法を含む Red Hat Satellite Server の保守方法について説明します。

6.1. ログとレポート機能

Red Hat Satellite は、システム情報を通知とログファイルの形式で提供します。

表6.1 報告およびトラブルシューティング向けのログファイル

ログファイル	ログファイルの内容の説明
/var/log/candlepin	サブスクリプションの管理
/var/log/foreman	Foreman
/var/log/foreman-proxy	Foreman プロキシー
/var/log/httpd	Apache HTTP サーバー
/var/log/foreman-installer/satellite	Satellite インストーラー
/var/log/foreman-installer/capsule	Capsule Server インストーラー
/var/log/libvirt	仮想化 API
/var/log/mongodb	Satellite データベース
/var/log/pulp	Celerybeat および Celery 起動要求メッセージ。起動が完了したら、メッセージは **/var/log/messages** に記録されます。
/var/log/puppet	設定管理
/var/log/rhsm	サブスクリプションの管理
/var/log/tomcat6 と **/var/log/tomcat**	それぞれ Red Hat Enterprise Linux 6 と Red Hat Enterprise Linux 7 向けの Apache Web サーバーメッセージ。
/var/log/messages	pulp、rhsm、および goferd に関連する他のさまざまなログメッセージ。

foreman-tail コマンドを使用して、Satellite に関連する多くのログファイルを追跡することもできます。**foreman-tail -l** を実行すると、追跡するプロセスとサービスがリストされます。

Red Hat Enterprise Linux 7 の場合は、*journal* を使用してより広範なロギング情報を得ることができます。詳細については、Using the Journal[3] を参照してください。

6.2. デバッグロギングの有効化

本項では、*デバッグロギング*を有効にして Satellite 6.2 の詳細なデバッグ情報を提供する方法について説明します。デバッグロギングにより、最も詳細なログ情報が提供され、Satellite 6.2 とそのコンポーネントで発生する可能性がある問題のトラブルシューティングが簡単になります。また、特定のロギングのために個別ロガーを有効または無効にすることもできます。

デバッグロギングを有効にするには、**/etc/foreman/settings.yaml** ファイルを変更します。

1. **ロギングレベルを "debug" に設定**
   デフォルトでは、ロギングレベルは以下のように **info** に設定されます。

   ```
   :logging:
     :level: info
   ```

   これらの行を以下のように変更します。

   ```
   :logging:
     :level: debug
   ```

   警告

   BZ#1325939 が解決されるまで、sql ロギングレベルを **error** に設定することは推奨されません。

2. **個別ロギングタイプの選択**
   デフォルトでは、**/etc/foreman/settings.yaml** の最後は以下のようになります。

   ```
   # Individual logging types can be toggled on/off here
   :loggers:
   ```

   /etc/foreman/settings.yaml ファイルを以下のように変更します。

   ```
   :loggers:
     :ldap:
       :enabled: true
     :permissions:
       :enabled: true
     :sql:
       :enabled: true
   ```

3. **Katello サービスの再起動**

   ```
   # katello-service restart
   ```

ロガーとそのデフォル値の完全なリスト

```
:app:
```

```
    :enabled: true
:ldap:
    :enabled: false
:permissions:
    :enabled: false
:sql:
    :enabled: false
```

6.3. ログファイルからの情報の収集

ログファイルから情報を収集するには以下の 2 つのユーティリティーがあります。

表6.2 ログ収集ユーティリティー

コマンド	説明
foreman-debug	**foreman-debug** コマンドは、Red Hat Satellite とそのバックエンドサービスの設定およびログファイルデータとシステム情報を収集します。この情報は収集され、tar ファイルに書き込まれます。 デフォルトでは、出力された tar ファイルは **/tmp/*foreman-debug-xxx.tar.xz*** にあります。詳細については、**foreman-debug --help** を実行します。 このコマンドの実行時はタイムアウトがありません。
sosreport	**sosreport** コマンドは、Red Hat Enterprise Linux システムから設定および診断情報 (実行中のカーネルバージョン、ロードされたモジュール、システムおよびサービス設定ファイルなど) を収集するツールです。また、このコマンドは外部プログラムを実行して (たとえば、**foreman-debug -g**)、Satellite 固有の情報を収集し、この出力を tar ファイルに格納します。 デフォルトでは、出力 tar ファイルは **/var/tmp/*sosreport-XXX-20171002230919.tar.xz*** にあります。詳細については、**sosreport --help** を実行するか、https://access.redhat.com/solutions/3592: 『What is a sosreport and how can I create one?』 を参照してください。 **sosreport** コマンドは **foreman-debug -g** を呼び出し、500 秒後にタイムアウトします。Satellite Server のログファイルが大きい場合や多くの Satellite タスクがある場合、サポートエンジニアはサポートケースを作成するときに **sosreport** と **foreman-debug** の出力を必要とすることがあります。

重要

foreman-debug と **sosreport** では、情報を収集する間にパスワード、トークン、キーなどのセキュリティー情報が削除されます。ただし、tar ファイルには依然として Red Hat Satellite Server についての機密情報が含まれる可能性があります。Red Hat は、この情報はパブリックではなく特定の受信者に直接送信することを推奨します。

6.4. サポートケースでのログファイルの使用

本章で説明されたログファイルと他の情報を使用して独自にトラブルシューティングを行ったり、サポートが必要な場合は、これらの情報と他の多くのファイルとともに診断および設定情報を取得して Red Hat サポートに送信したりできます。

Red Hat サポートでサポートケースを作成するには 2 つの方法があります。サポートケースは、Satellite Web UI またはカスタマーポータルから直接作成できます。

- 「Red Hat Access プラグインを使用したサポートケースの作成」: Satellite Web UI からのサポートケースの作成方法
- https://access.redhat.com/articles/38363: 『カスタマーポータルでのサポートケースの作成および管理方法』

6.5. RED HAT SATELLITE からのカスタマーポータルサービスへのアクセス

Red Hat Access の事前インストール済みプラグインを使用すると、Satellite Web UI 内から複数の Red Hat カスタマーポータルサービスにアクセスできます。

Red Hat Access プラグインは以下のサービスを提供します。

- **Search: (検索:)** Satellite Web UI 内からカスタマーポータルのソリューションを検索します。
- **Logs: (ログ:)** 問題解決に役に立つログファイルの特定の部分 (スニペット) を送信します。これらのログスニペットは Red Hat カスタマーポータルの診断ツールチェーンに送信します。
- **Support: (サポート:)** Satellite Web UI 内で、作成されたサポートケースにアクセスしたり、作成されたサポートケースを変更したり、新しいサポートケースを作成したりします。

注記

Red Hat カスタマーポータルのリソースにアクセスするには、Red Hat カスタマーポータルのユーザー ID とパスワードを使ってログインする必要があります。

6.5.1. Red Hat Access プラグインでのソリューションの検索

Red Hat Access プラグインは、Red Hat カスタマーポータルで利用できるソリューションデータベースを参照する検索機能を提供します。

手順6.1 Red Hat Satellite Server からのソリューションの検索:

1. 右上で **Red Hat Access → Search (検索)** をクリックします。
2. 必要な場合は、Red Hat カスタマーポータルにログインします。右上のメインパネルで Log In (ログイン) をクリックします。

注記

Red Hat カスタマーポータルのリソースにアクセスするには、Red Hat カスタマーポータルのユーザー ID とパスワードを使ってログインする必要があります。

3. **Red Hat Search** フィールドに検索クエリーを入力します。検索結果が左側の **Recommendations (推奨項目)** リストに表示されます。

4. **Recommendations (推奨項目)** リストでソリューションをクリックします。ソリューションの記事がメインパネルに表示されます。

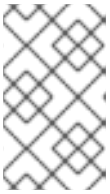
6.5.2. Red Hat Access プラグインでのログの使用

ログファイルビューアーを使用すると、ログファイルを表示し、ログの一部を分離できます。また、カスタマーポータルの診断ツールでログの一部を送信して、問題解決のサポートを受けることもできます。

手順6.2 Red Hat Satellite サーバーからのログ診断ツールの使用:

1. 右上で **Red Hat Access → Logs (ログ)** をクリックします。

2. 必要な場合は、Red Hat カスタマーポータルにログインします。右上のメインパネルで **Log In (ログイン)** をクリックします。



注記

Red Hat カスタマーポータルのリソースにアクセスするには、Red Hat カスタマーポータルのユーザー ID とパスワードを使ってログインする必要があります。

3. 左側にあるファイルツリーで、ログファイルを選択し、ファイル名をクリックします。

4. **Select File (ファイルの選択)** をクリックします。ポップアップウィンドウには、ログファイルの内容が表示されます。

5. ログファイルで、診断するテキストセクションを強調表示します。**Red Hat Diagnose (Red Hat 診断)** ボタンが表示されます。

6. **Red Hat Diagnose (Red Hat 診断)** をクリックします。これにより、強調表示された情報が Red Hat カスタマーポータルに送信され、提供されたログ情報に近似するソリューションが提供されます。

7. 以下のケースに従います。

   - ソリューションが問題に一致する場合は、ソリューションをクリックし、必要な手順を実行して問題のトラブルシューティングを行います。

   - ソリューションが問題に一致しない場合は、**Open a New Support Case (サポートケースを新規作成)** をクリックします。サポートケースには、ログファイルの強調表示されたテキストが入力されます。「Red Hat Access プラグインを使用したサポートケースの作成」 を参照してください。

6.5.3. Red Hat Access プラグインを使用した既存サポートケースの表示

Red Hat Access プラグインを使用すると、Red Hat Satellite Server から既存のサポートケースを表示できます。

手順6.3 Red Hat Satellite サーバーからの既存サポートケースの表示:

1. 右上で **Red Hat Access → Support (サポート) → My Cases (自分のケース)** をクリックします。
2. 必要な場合は、Red Hat カスタマーポータルにログインします。右上のメインパネルで **Log In (ログイン)** をクリックします。

注記

Red Hat カスタマーポータルのリソースにアクセスするには、Red Hat カスタマーポータルのユーザー ID とパスワードを使ってログインする必要があります。

3. 以下のいずれかを実行し、既存のケースの中から特定のサポートケースを検索します。
    1. **Search (検索)** フィールドにキーワードまたはフレーズを入力します。
    2. ドロップダウンリストから、特定の **Case Group (ケースグループ)** を選択します。**Case Groups (ケースグループ)** は、ユーザーの組織により Red Hat カスタマーポータル内で定義されています。
    3. ケースのステータスを選択します。
4. 検索結果から特定のサポートケースを選択し、**Case ID (ケース ID)** をクリックします。サポートケースは表示できます。

6.5.4. Red Hat Access プラグインを使用したサポートケースの変更

Red Hat Access プラグインを使用すると、Red Hat Satellite Server から既存のサポートケースを更新できます。

手順6.4 Red Hat Satellite Server Web UI からのサポートケースの更新:

1. 「Red Hat Access プラグインを使用した既存サポートケースの表示」 の手順を完了します。
2. サポートケースで、マークされたセクションにスクロールダウンし、以下のことを行います。
    - **Attachments: (添付ファイル:)** - システムにあるローカルファイルを添付します。ファイル名を追加して識別しやすくします。

注記

ファイル名は 80 文字未満にしてください。Web UI を使用してアップロードする添付ファイルの最大サイズは 250 MBです。ファイルのサイズがそれよりも大きい場合は、FTP を使用します。

    - **Case Discussion: (ケースディスカッション:)** - グローバルサポートサービスに相談するケースに関する更新情報を追加します。情報の追加後に **Add Comment (コメントの追加)** をクリックします。

6.5.5. Red Hat Access プラグインを使用したサポートケースの作成

Red Hat Access プラグインを使用して、Red Hat Satellite Server から新規サポートケースを作成できます。

手順6.5 Red Hat Satellite Server を使用した新規サポートケースの作成:

1. 右上にある **Red Hat Access → Support (サポート) → New Case (新規ケース)** をクリックします。
2. 必要な場合は、Red Hat カスタマーポータルにログインします。右上のメインパネルで Log In (ログイン) をクリックします。

注記

Red Hat カスタマーポータルのリソースにアクセスするには、Red Hat カスタマーポータルのユーザー ID とパスワードを使ってログインする必要があります。

3. **Product (製品)** フィールドと **Product Version (製品バージョン)** フィールドにデータが自動的に設定されます。以下のように他の関連フィールドにデータを入力してください。
   - **Summary (概要)** — 問題の簡単な概要を記載します。
   - **Description (詳細)** — 問題の詳細を記載します。

   提供した概要に基づいて、推奨されるソリューションがメインパネルに表示されます。
4. **Next (次へ)** をクリックします。
5. 以下のように適切なオプションを選択します。
   - **Severity (重大度)** — チケットの緊急度に応じて 4 (低)、3 (通常), 2 (高)、または 1 (緊急) を選択します。
   - **Case Group (ケースグループ)** — 通知の必要なメンバーに応じて、サポートケースに関連付けられたケースグループを作成します。Red Hat Satellite でケースグループを選択します。カスタマーポータル内でケースグループを作成します。
6. **sosreport** の出力と必要なファイルを添付します。ファイルの詳細を追加し、**Attach (添付)** をクリックします。

注記

- 大規模なログファイルまたは多くの Satellite タスクがある場合は、**foreman-debug** の出力も添付することが推奨されます。
- ファイル名は 80 文字未満にしてください。Web UI を使用してアップロードする添付ファイルの最大サイズは 250 MBです。ファイルのサイズがそれ以上の場合は、FTP を使用します。

7. **Submit (送信)** をクリックします。システムによりケースがカスタマーポータルにアップロードされ、参考のためにケース番号が提供されます。

Red Hat ナレッジベース記事である https://access.redhat.com/articles/445443: 『Red Hat Access: Red Hat Support Tool』 には、追加情報、例、および動画チュートリアルが含まれます。

6.6. SATELLITE SERVER での RED HAT INSIGHTS の使用

Red Hat Insights を使用すると、セキュリティー 違反、パフォーマンスの低下、および安定性の消失

に関連するシステムとダウンタイムを積極的に診断できます。ダッシュボードを使用して、安定性、セキュリティー、またはパフォーマンスの主要なリスクを素早く特定できます。また、カテゴリー別に分類したり、影響度および解決方法の詳細を表示したり、影響を受けたシステムを調べたりすることができます。

Red Hat Insights は、デフォルトで Satellite Server にインストールされます。Insights を Satellite Server で使用する前に、Red Hat Insights に移動して、**Satellite 6** をクリックして事前インストールチェックを行ったり、Satellite Server を登録したりします。

6.7. WEB UI での SATELLITE SERVER の監視

Satellite Server Web UI の **About （概要）**ページで、以下の概要情報を見つけることができます。

- システムステータス (Capsule、利用可能なプロバイダー、コンピュートリソース、およびプラグインを含む)
- サポート情報
- システム情報
- バックエンドシステムの状態
- インストールされたパッケージ

About （概要）ページに移動します。

- Satellite Server Web UI の右上隅で **Administer (管理) → About (概要)** をクリックします。

---

[3] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/s1-Using_the_Journal.html

第7章 CAPSULE SERVER の監視

以下の項では、Satellite Web UI を使用して、保守とトラブルシューティングに役に立つ Capsule 情報を見つける方法について説明します。

7.1. 一般的な CAPSULE 情報の表示

Infrastructure (インフラストラクチャー) → Capsules に移動して、Satellite Server に登録された Capsule Server の表を表示します。表に含まれる情報には以下の質問に対する回答が含まれます。

Capsule Server が実行されているか?

これは、**Status (ステータス)** 列で緑色のアイコンにより示されます。赤色のアイコンは、非アクティブな Capsule を示します。その Capsule をアクティベートするためにするには、Capsule Server で **service foreman-proxy restart** コマンドを使用します。

どのサービスが Capsule Server で有効であるか?

Features (機能) 列で、Capsule がたとえば DHCP サービスを提供するかどうかや Pulp ノードとして動作するかどうかを確認できます。Capsule の機能はインストール中に有効にしたり、後で設定したりできます。詳細については、Red Hat Satellite Installation Guide を参照してください。

Capsule Server はどの組織およびロケーションに割り当てられたか?

Capsule サーバーは複数の組織およびロケーションに割り当てることができますが、現在選択された組織に属する Capsule のみが表示されます。すべての Capsule をリストするには、左上隅にあるコンテキストメニューから **Any Organization (任意の組織)** を選択します。

Capsule 設定の変更後に、**Actions (アクション)** 列のドロップダウンメニューから **Refresh (更新)** を選択して Capsule の表を最新状態にしてください。

詳細情報を表示するには Capsule 名をクリックします。**Overview (概要)** タブでは、Capsule の表にあるのと同じ情報を見つけることができます。さらに、以下の質問に回答することができます。

どのホストが Capsule Server によって管理されているか?

関連するホストの数は **Hosts managed (管理対象ホスト数)** ラベルの横に表示されます。関連するホストの詳細を表示するには、その数をクリックします。

どれくらいのストレージ容量が Capsule Server で利用可能であるか?

/var/lib/pulp、**/var/lib/pulp/content**、および **/var/lib/mongodb** で Pulp コンテンツにより使用されたストレージ容量が表示されます。また、Capsule で利用可能な残りのストレージ容量を確認できます。

7.2. サービスの監視

Infrastructure (インフラストラクチャー) → Capsules に移動して、選択された Capsule の名前をクリックします。**Services (サービス)** タブでは、DNS ドメインのリストや Pulp ワーカーの数などの、Capsule サービスに関する基本的な情報を見つけることができます。ページの外観は、Capsule Server で有効なサービスによって異なります。より詳細なステータス情報を提供するサービスには Capsule ページで専用のタブが用意されることがあります (「Puppet の監視」 を参照)。

7.3. PUPPET の監視

Infrastructure (インフラストラクチャー) → Capsules に移動して、選択された Capsule の名前をクリックします。**Puppet** タブでは、以下の情報を見つけることができます。

- **General（全般）**サブタブの Puppet イベントの概要、最新の Puppet 実行の概要、関連するホストの同期ステータス 。
- **Environments（環境）**サブタブの Puppet 環境のリスト。

Puppet CA タブでは、以下の情報を見つけることができます。

- **General（全般）**サブタブの証明書ステータスの概要と自動署名エントリーの数。
- **Certificates（証明書）**サブタブの Capsule に関連する CA 証明書の表。ここでは、証明書失効データを調べたり、**Revoke（取り消し）**をクリックして証明書をキャンセルしたりできます。
- **Autosign entries（自動署名エントリー）**サブタブの自動署名エントリーのリスト。ここでは、**New（新規）**をクリックしてエントリーを作成したり、**Delete（削除）**をクリックしてエントリーを削除したりできます。

第8章 外部認証の設定

外部認証を使用することにより、外部 ID プロバイダーのユーザーグループメンバーシップからユーザーとユーザーグループのパーミッションを派生させることができます。したがって、これらのユーザーを作成したり、グループメンバーシップを Satellite Server で手動で保守したりする必要はありません。Red Hat Satellite では、外部認証を設定する 4 つの一般的なシナリオがサポートされます。

- **Lightweight Directory Access Protocol** (LDAP) サーバーを外部 ID プロバイダーとして使用するシナリオ。LDAP は、一元的に保存された情報にネットワークを介してアクセスするために使用されるオープンプロトコルセットです。詳細については、「LDAP を使用」 を参照してください。LDAP を使用して IdM または AD サーバーに接続できますが、セットアップでは、Satellite の Web UI でのサーバー検出、フォレスト間信頼、または Kerberos を使用したシングルサインオンがサポートされません。

- **Red Hat Enterprise Linux Identity Management** (IdM) サーバーを外部 iD プロバイダーとして使用するシナリオ。IdM は、ネットワーク環境で使用される個別 ID、クレデンシャル、および権限を管理します。詳細については、「ID 管理の使用」 を参照してください。

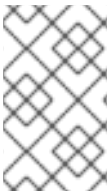
- フォレスト間 Kerberos 信頼を介して IdM に統合された **Active Directory** (AD) を外部 ID プロバイダーとして使用するシナリオ。詳細については、「フォレスト間信頼での Active Directory の使用」 を参照してください。

- 直接 AD を外部 ID プロバイダーとして使用するシナリオ。詳細については、「Active Directory の直接的な使用」 を参照してください。

上記のシナリオでは、Satellite Server にアクセスを提供します。また、Satellite でプロビジョニングされたホストを IdM レルムと統合することもできます。Red Hat Satellite には、レルムまたはドメインプロバイダーに登録されたシステムのライフサイクルを自動的に管理するレルム機能があります。詳細については、「プロビジョンされたホストの外部認証」 を参照してください。

8.1. LDAP を使用

8.1.1. TLS での セキュア LDAP (LDAPS) の設定



注記

本項では直接 LDAP 統合について説明しますが、Red Hat は SSSD を使用し、IdM、AD、または LDAP サーバーに対して SSSD を設定することをお勧めします。これらの優先される設定については、本書の他の箇所で説明します。

Red Hat Satellite で **TLS** を使用してセキュアな LDAP 接続 (LDAPS) を確立する必要がある場合は、最初に、接続する LDAP サーバーで使用された証明書を使用し、以下で説明しているように Satellite Server のベースオペレーティングシステムでそれらの証明書を信頼済みとして指定します。LDAP サーバーで中間認証局との証明書チェーンが使用される場合は、すべての証明書を取得するためにチェーンのすべてのルートおよび中間証明書が信頼済みである必要があります。この時点でセキュアな LDAP を必要としない場合は、手順8.1「LDAP 認証の設定:」 に進みます。

LDAP サーバーからの証明書の取得
Active Directory 証明書サービスを使用する場合は、ベース 64 エンコード X.509 形式を使用してエンタープライズ PKI CA 証明書をエクスポートします。Active Directory サーバーでの CA 証明書の作成およびエクスポートについては、How to configure Active Directory authentication with**TLS** on Satellite 6.2 を参照してください。

LDAP サーバー証明書を、Satellite Server がインストールされた Red Hat Enterprise Linux システ

ム上の一時的な場所にダウンロードし、作業が終了したら削除します (たとえば、**/tmp/example.crt**)。ファイル名拡張子 **.cer** と **.crt** は慣習にすぎず、DER バイナリーまたは PEM ASCII 形式の証明書を示すことがあります。

LDAP サーバーからの証明書を信頼する
Red Hat Satellite Server では、LDAP 認証用の CA 証明書は **/etc/pki/tls/certs/** ディレクトリー内の個別ファイルである必要があります。

install コマンドを使用して適切なパーミッションでインポート済み証明書を **/etc/pki/tls/certs/** ディレクトリーにインストールします。

```
# install /tmp/example.crt /etc/pki/tls/certs/
```

root で以下のコマンドを入力して LDAP サーバーから取得された *example.crt* 証明書を信頼します。

```
# ln -s example.crt /etc/pki/tls/certs/$(openssl x509 -noout -hash -in
/etc/pki/tls/certs/example.crt).0
```

httpd サービスを再起動します。

- Red Hat Enterprise Linux 6 の場合:

  ```
  # service httpd restart
  ```

- Red Hat Enterprise Linux 7 の場合:

  ```
  # systemctl restart httpd
  ```

8.1.2. LDAP を使用するよう Red Hat Satellite を設定

Web UI を使用して LDAP 認証を設定するには以下の手順を実行します。Satellite の Web UI で Kerberos を使用したシングルサインオン機能が必要な場合は、代わりに IdM および AD 外部認証を使用する必要があることに注意してください。これらのオプションの詳細については、「ID 管理の使用」 または 「Active Directory の使用」 を参照してください。

手順8.1 LDAP 認証の設定:

1. 許可 Network Information System (NIS) サービスのブール値を true に設定して SELinux により送信 LDAP 接続が中止されるのを防ぎます。

   - Red Hat Enterprise Linux 6 の場合

     ```
     # setsebool -P allow_ypbind on
     ```

   - Red Hat Enterprise Linux 7 の場合

     ```
     # setsebool -P nis_enabled on
     ```

2. **Administer (管理) → LDAP Authentication (LDAP 認証)** に移動します。
3. **New authentication source (新規の認証ソース)** をクリックします。
4. **LDAP server (LDAP サーバー)** タブで LDAP サーバーの名前、ホスト名、ポート、および

サーバータイプを入力します。デフォルトポートは 389、デフォルトサーバータイプは POSIX (認証サーバーのタイプに応じて FreeIPA または Active Directory を選択することもできます)。**TLS** 暗号化接続に対しては、**LDAPS** チェックボックスを選択して暗号化を有効にします。ポートは LDAPS のデフォルト値である 636 に変更されるはずです。

5. **Account (アカウント)** タブでアカウント情報とドメイン名の詳細を入力します。説明と例については、「LDAP 設定の説明と例」 を参照してください。

6. **Attribute mappings (マッピング属性)** タブで LDAP 属性を Satellite 属性にマップします。ログイン名、名、姓、電子メールアドレス、および写真の属性をマップできます。例については、「LDAP 設定の説明と例」 を参照してください。

7. **送信** をクリックします。

この時点で Satellite Server は LDAP サーバーを使用するよう設定されました。**Automatically create accounts in Satellite (Satellite でアカウントを自動作成)** を選択しなかった場合は、「ユーザーの作成」 を算用してユーザーアカウントを手動で作成します。そのオプションを選択した場合、LDAP ユーザーは LDAP アカウントおよびパスワードを使用して Satellite にログインできます。最初にログインしたあとに、個別ユーザーアカウントを組織とロールを割り当てることができます。または、ユーザーアカウントを組織に自動的に関連付けるために、**Administer (管理) → Organizations (組織)** に移動します。組織を選択し、**User (ユーザー)** タブをクリックして、**All users (すべてのユーザー)** を選択します。ロールは手動で割り当てる必要があります。Satellite でユーザーアカウントに適切なロールを割り当てるには、「ユーザーへのロールの割り当て」 を参照してください。

8.1.3. LDAP 設定の説明と例

以下の表は、**Account (アカウント)** タブの各設定の説明を示しています。

表8.1 Account (アカウント) タブの設定

設定	説明
Account username (アカウントユーザー名)	LDAP サーバーへの読み取りアクセスを持つ LDAP ユーザー。ユーザー名は、サーバーで匿名の読み取りが許可されている場合は必要ありません。許可されていない場合は、ユーザーのオブジェクトへの完全パスを使用します。以下に例を示します。 `uid=$login,cn=users,cn=accounts,dc=example,dc=com` **$login** 変数には、ログインページで入力されたユーザー名がリテラル文字列として格納されます。この値は、変数が展開されたときにアクセスされます。 この変数は、LDAP ソースからの外部ユーザーグループとは使用できません。ユーザーがログインしていない場合、Satellite はグループリストを取得する必要があります。匿名または専用サービスユーザーを使用してください。
Account password (アカウントパスワード)	**Account username (アカウントユーザー名)** フィールドで定義されたユーザーの LDAP パスワード。**Account username (アカウントユーザー名)** が **$login** 変数を使用している場合は、このフィールドを空白のままにすることができます。
Base DN	LDAP ディレクトリーの最上位のドメイン名。

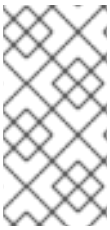
設定	説明
Groups base DN (グループベース DN)	グループが含まれる LDAP ディレクトリーツリーの最上位のドメイン名。
LDAP filter (LDAP フィルター)	LDAP クエリーを制限するフィルター。
Automatically create accounts in Satellite (Satellite でアカウントを自動作成)	このオプションが選択された場合は、LDAP ユーザーが初めて Satellite にログインしたときに、Satellite ユーザーアカウントが自動的に作成されます。**Permissions Denied** 警告が表示されます。ユーザーは Satellite 管理者に連絡してユーザーアカウントにロールを関連付けてもらう必要があります。
Usergroup sync (ユーザーグループの同期)	このオプションが選択された場合は、ユーザーがログインしたときにユーザーのユーザーグループメンバーシップが自動的に同期されます。これにより、メンバーシップは常に最新の状態になります。このオプションが選択されない場合は、Satellite で Cron ジョブを使用してグループメンバーシップを定期的 (デフォルトでは 30 分ごと) に同期します。詳細については、手順8.6「外部ユーザーグループの設定:」 を参照してください。

以下の表は、異なる種類の LDAP 接続の設定例を示しています。以下のすべての例では、ユーザーおよびグループのエントリーに対してバインド、読み取り、および検索のパーミッションを持つ **redhat** という名前の専用サービスアカウントを使用します。LDAP 属性名では大文字と小文字が区別されることに注意してください。

表8.2 Active Directory LDAP 接続の設定例

設定	値例
アカウントユーザー名	DOMAIN\redhat
アカウントパスワード	P@ssword
ベース DN	DC=example,DC=COM
グループベース DN	CN=Users,DC=example,DC=com
ログイン名属性	userPrincipalName
名属性	givenName
ラストネーム属性	sn

設定	値例
メールアドレス属性	mail



注記

userPrincipalName では、ユーザー名にスペースを使用できます。ログイン名属性 **sAMAccountName** (上記の表にはリストされていない) は、レガシー Microsoft システムとの後方互換性を提供します。**sAMAccountName** では、ユーザー名にスペースを使用できません。

表8.3 FreeIPA または Red Hat Identity Management LDAP 接続の設定例

設定	値例
アカウントユーザー名	uid=redhat,cn=users,cn=accounts,dc=example,dc=com
ベース DN	dc=example,dc=com
グループベース DN	cn=groups,cn=accounts,dc=example,dc=com
ログイン名属性	uid
名属性	givenName
ラストネーム属性	sn
メールアドレス属性	mail

表8.4 POSIX (OpenLDAP) LDAP 接続の設定例

設定	値例
アカウントユーザー名	uid=redhat,ou=users,dc=example,dc=com
ベース DN	dc=example,dc=com
グループベース DN	cn=employee,ou=userclass,dc=example,dc=com
ログイン名属性	uid
名属性	givenName
ラストネーム属性	sn

設定	値例
メールアドレス属性	mail

8.2. ID 管理の使用

以下の方法のいずれかを選択します。

- 「ID 管理の直接的な使用」
- 「LDAP 認証での ID 管理の使用」

8.2.1. ID 管理の直接的な使用

本項では、Red Hat Satellite Server と IdM サーバーを統合する方法とホストベースアクセス制御を有効にする方法を示します。

前提条件
Satellite Server は Red Hat Enterprise Linux 7.1 または Red Hat Enterprise Linux 6.6 以降で実行する必要があります。

本章の例では、IdM と Satellite の設定が分かれていることを前提とします。ただし、両方のサーバーに対して管理者権限を持っている場合は、Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy Guide[4] で説明されているように、IdM を設定できます。

Satellite Server のベースオペレーティングシステムは、組織の IdM 管理者によって IdM ドメインに登録されている必要があります。

手順8.2 Satellite Server での IdM 認証の設定:

1. 以下のように、IdM サーバー上で Satellite Server のホストエントリーを作成し、ワンタイムパスワードを生成します。

```
# ipa host-add --random hostname
```

注記

IdM 登録を完了するには、生成されたワンタイムパスワードをクライアントで使用する必要があります。

ホスト設定プロパティーの詳細については、Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy Guide[5] を参照してください。

2. 以下のように、Satellite Server 向けの HTTP サービスを作成します。

```
# ipa service-add servicename/hostname
```

サービスの管理の詳細については、Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy Guide[6] を参照してください。

3. Satellite Server で、IdM 登録を設定するために、root で以下のコマンドを実行します。

```
# ipa-client-install --password OTP
```

OTP を、IdM 管理者により提供されたワンタイムパスワードに置き換えます。

4. Satellite Server が Red Hat Enterprise Linux 7 上で実行されている場合は、以下のコマンドを実行します。

```
# subscription-manager repos --enable rhel-7-server-optional-rpms
```

インストーラーは、オプションのリポジトリー **rhel-7-server-optional-rpms** (Red Hat Enterprise Linux 7 の場合) に含まれるパッケージに依存します。Red Hat Enterprise Linux 6 の場合、必要なすべてのパッケージは **base** リポジトリーに含まれます。

5. 以下のコマンドを実行します。

```
# satellite-installer --foreman-ipa-authentication=true
```

このコマンドは、Satellite のフレッシュインストールに限定されません。既存の Satellite インストールを変更するためにも使用できます。

6. Katello サービスを再起動します。

```
# katello-service restart
```

この時点で、外部ユーザーは IdM クレデンシャルを使用して Satellite にログインできます。この場合、ユーザー名とパスワードを使用して直接 Satellite Server にログインするか、設定された Kerberos シングルサインオンを利用し、クライアントマシンでチケットを取得して、自動的にログインすることを選択できます。また、ワンタイムパスワードを使用した 2 要素認証 (2FA OTP) もサポートされます。IdM 内のユーザーが 2FA 向けに設定され、Satellite Server が Red Hat Enterprise Linux 7 上で実行されている場合、このユーザーは OTP で Satellite に対して認証することもできます。オプションで、次の手順に進んでホストベースアクセス制御 (HBAC) を設定します。

HBAC ルールでは、IdM ユーザーがアクセスすることを許可されたドメイン内のマシンを定義します。選択されたユーザーが Satellite Server にアクセスすることを防ぐよう IdM サーバー上で HBAC を設定できます。この方法では、ログインが許可されないユーザーのデータベースエントリーを Satellite が作成することを防ぐことができます。HBAC の詳細については、Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy Guide[7] を参照してください。

手順8.3 HBAC の設定:

1. HBAC サービスおよびルールを IdM サーバーで作成し、リンクします。以下の例では、**satellite-prod** という PAM サービス名を使用しています。IdM サーバー上で以下のコマンドを実行してください。

```
$ ipa hbacsvc-add satellite-prod
$ ipa hbacrule-add allow_satellite_prod
$ ipa hbacrule-add-service allow_satellite_prod --
hbacsvcs=satellite-prod
```

2. サービス satellite-prod へのアクセスを持つユーザーと Satellite Server のホスト名を追加します。

```
$ ipa hbacrule-add-user allow_satellite_prod --user=username
$ ipa hbacrule-add-host allow_satellite_prod --hosts=the-satellite-fqdn
```

または、**allow_satellite_prod** ルールにホストグループとユーザーグループを追加します。

3. ルールのステータスを確認するために、以下のコマンドを実行します。

```
$ ipa hbacrule-find satellite-prod
$ ipa hbactest --user=username --host=the-satellite-fqdn --service=satellite-prod
```

4. IdM サーバーで allow_all rule が無効であることを確認します。他のサービスに影響を与えずにこれを行う方法については、How to configure HBAC rules in IdMarticle on the Red Hat Customer Portal[8] を参照してください。

5. 手順8.2「Satellite Server での IdM 認証の設定:」で説明されているように、Satellite Server で IdM 統合を設定します。Satellite Server で、root として PAM サービスを定義します。

```
# satellite-installer --foreman-pam-service=satellite-prod
```

8.2.2. LDAP 認証での ID 管理の使用

シングルサインオンサポートなしで外部認証ソースとして ID 管理を使用する場合の詳細については、「LDAP を使用」 を参照してください。

8.3. ACTIVE DIRECTORY の使用

以下の方法のいずれかを選択します。

- 「フォレスト間信頼での Active Directory の使用」
- 「Active Directory の直接的な使用」
- 「LDAP 認証での Active Directory の使用」

8.3.1. フォレスト間信頼での Active Directory の使用

Kerberos を使用すると、2 つの異なるドメインフォレスト間の関係を定義する**フォレスト間信頼**を作成できます。ドメインフォレストはドメインの階層構造です。フォレストは AD と IdM によって形成されます。AD と IdM との間で有効な信頼関係により、AD のユーザーは一連のクレデンシャルを使用して Linux ホストおよびサービスにアクセスできます。フォレスト間信頼の詳細については、Red Hat Enterprise Linux Windows Integration Guide[9] を参照してください。

Satellite の観点から、設定プロセスは、フォレスト間信頼を設定せずに IdM サーバーと統合することと同じです。Satellite Server は IPM ドメインで登録し、「ID 管理の使用」 で説明されているように統合する必要があります。IdM サーバーで、以下の追加の手順を実行する必要があります。

1. HBAC 機能を有効にするために、外部グループを作成し、AD グループをその外部グループに追加します。新しい外部グループを POSIX グループに追加します。この POSIX グループを HBAC ルールで使用します。

2. AD ユーザーの追加属性を転送するよう sssd を設定します。これらの属性を **/etc/sssd/sssd.conf** の **nss** セクションと **domain** セクションに追加します。

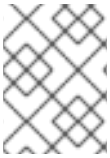
```
[nss]
user_attributes=+mail, +sn, +givenname

[domain/EXAMPLE]
ldap_user_extra_attrs=mail, sn, givenname
```

8.3.2. Active Directory の直接的な使用

本項では、直接 Active Directory (AD) を Satellite Server の外部認証ソースとして使用する方法を示します。直接 AD 統合は、Satellite Server が、ID が格納された AD ドメインに直接参加することを意味します。推奨されるセットアップは 2 つの手順から構成され、最初に 手順8.4「AD サーバーを使用した Satellite Server の登録:」 で説明されているように AD を使用して Satellite を登録し、次に 手順8.5「GSS-proxy との直接 AD 統合の設定:」 で説明されているように GSS-proxy を使用して AD 統合を完了します。

Apache での Kerberos 認証の従来のプロセスでは、Apache プロセスが keytab ファイルへの読み取りアクセスを持っている必要があります。GSS-Proxy を使用すると、Kerberos 認証機能を保持しつつ keytab ファイルへのアクセスを削除することにより Apache サーバーに対してより厳密な権限の分離を行えます。AD を Satellite の外部認証ソースとして使用する場合は、keytab ファイルのキーがホストキーと同じであるため、GSS-proxy を実装することが推奨されます。



注記

AD 統合では、Red Hat Satellite Server を Red Hat Enterprise Linux 7.1 上にデプロイする必要があります。

Satellite Server のベースオペレーティングシステムとして動作する Red Hat Enterprise Linux で以下の手順を実行します。本項の例では、*EXAMPLE.ORG* が AD ドメインの Kerberos レルムです。手順を完了すると、EXAMPLE.ORG レルムに属するユーザーは Satellite Server にログインできます。

前提条件
GSS-proxy と nfs-utils をインストールします。

```
# yum install gssproxy nfs-utils
```

手順8.4 AD サーバーを使用した Satellite Server の登録:

1. 必要なパッケージをインストールします。

```
# yum install sssd adcli realmd ipa-python
```

2. AD サーバーを使用して Satellite Server を登録します。以下のコマンドを実行するには、管理者パーミッションが必要な場合があります。

```
# realm join -v EXAMPLE.ORG
```

AD サーバーを使用して Satellite を登録したら、**satellite-installer** コマンドを使用して GSS-proxy との直接 AD 統合を設定できます。これは、すでにインストールされた Satellite に対して、または Satellite のインストール中に行えます。Apache ユーザーは keytab ファイルへのアクセスを持

たない必要があることに注意してください。また、Apache ユーザーの実効ユーザー ID (**id apache** を実行して確認可能) をメモしてください。以下の手順では、例として UID **48** を使用します。

手順8.5 GSS-proxy との直接 AD 統合の設定:

1. デフォルトでは、**satellite-installer** コマンドが IdM 統合に設定されます。この設定を変更するには、以下の内容で **/etc/ipa/default.conf** ファイルを作成します。

```
[global]
server = unused
realm = EXAMPLE.ORG
```

2. 以下の内容で **/etc/net-keytab.conf** ファイルを作成します。

```
[global]
workgroup = EXAMPLE
realm = EXAMPLE.ORG
kerberos method = system keytab
security = ads
```

3. 以下のコマンドを使用して HTTP 向け keytab ファイルを作成します。

```
# KRB5_KTNAME=FILE:/etc/gssproxy/http.keytab net ads keytab add HTTP
-U administrator -d3 -s /etc/net-keytab.conf
```

このコマンドを実行すると、AD サーバーから HTTP サービス keytab ファイルが取得され、**/etc/gssproxy/http.keytab** に格納されます。このファイルは root ユーザーおよびグループによって所有されるようにしてください。

```
# chown root:root /etc/gssproxy/http.keytab
```

4. 以下の行を **/etc/krb5.conf** ファイルの先頭に挿入します。

```
includedir /var/lib/sss/pubconf/krb5.include.d/
```

5. **/etc/httpd/conf/http.keytab** に空の keytab ファイルを作成します。

```
# touch /etc/httpd/conf/http.keytab
```

6. 以下のコマンドを実行します。

```
# satellite-installer --foreman-ipa-authentication=true
```

7. **gssproxy** サービスを起動して、有効にします。

```
# systemctl restart gssproxy.service
# systemctl enable gssproxy.service
```

8. Apache サーバーが GSS-proxy を使用するよう設定するために。以下の内容で **/etc/systemd/system/httpd.service** ファイルを作成します。

```
.include /lib/systemd/system/httpd.service
[Service]
Environment=GSS_USE_PROXY=1
```

変更をサービスに適用します。

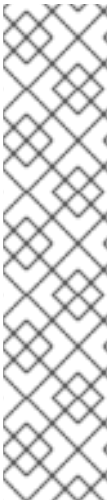
```
# systemctl daemon-reload
```

9. **httpd** サービスを起動し、有効にします。

```
# systemctl restart httpd.service
```

Apache サーバーが実行中であり、クライアントに有効な Kerberos チケットがある場合、サーバーに対して HTTP 要求を行うユーザーは認証されます。

この時点でユーザーは Satellite GUI でアクセスクレデンシャルを入力せずにブラウザーの Kerberos SSO がログインできるよう設定できます。Firefox ブラウザーの設定の詳細については、Red Hat Enterprise Linux System-Level Authentication Guide を参照してください。Internet Explorer ブラウザーのユーザーは、ローカルイントラネットまたは信頼できるサイトのリストに Satellite Server を追加し、**Enable Integrated Windows Authentication (統合 Windows 認証を使用する)** 設定を有効にします。詳細については、Internet Explorer のドキュメンテーションを参照してください。



注記

直接 AD 統合では、IdM を介した HBAC は利用できません。代わりに、管理者が AD 環境でポリシーを一元管理することを可能にする Group Policy Objects (GPO) を使用できます。GPO と PAM サービス間の適切なマッピングを行うには、以下の sssd 設定を使用します。

```
access_provider = ad
ad_gpo_access_control = enforcing
ad_gpo_map_service = +satellite-prod
```

ここで、**satellite-prod** は PAM サービス名です。GPO の詳細については、Red Hat Enterprise Linux Windows Integration Guide[10] を参照してください。

8.3.3. LDAP 認証での Active Directory の使用

シングルサインオンサポートなしで外部認証ソースとして Active Directory に接続する場合の詳細については、「LDAP を使用」 を参照してください。設定例については、How to configure Active Directory authentication with TLS on Satellite 6 を参照してください。

8.4. 外部ユーザーグループの設定

外部ソースを介して認証されたユーザーは、最初にログインしたときに Satellite Server で自動的に作成されます。これは、Satellite GUI で手動で作成されたユーザーグループにマップする必要がある外部ユーザーグループには適用されません。外部ユーザーグループのメンバーは、自動的に Satellite ユーザーグループのメンバーになり、関連するパーミッションを受け取ります。

前提条件
外部ユーザーグループの設定は、外部認証の種類によって異なります。

- LDAP ソースを使用している場合は、LDAP 認証が適切に設定されていることを確認します。**Administer (管理) → LDAP Authentication (LDAP 認証)** に移動して、既存のソースを参照および変更します。LDAP ソースの作成手順については、「LDAP を使用」 を参照してください。使用する LDAP グループ名をメモします。

注記

LDAP ソースから外部ユーザーグループを使用している場合は、アカウントユーザー名の代わりに **$login** 変数を使用できません。匿名または専用サービスユーザーを使用する必要があります。

- *8章 外部認証の設定* で説明されたように Satellite が IdM または AD サーバーで登録されている場合は、使用する外部ユーザーグループをメモします。外部ユーザーのグループメンバーシップを見つけるには、Satellite で **id** コマンドを実行します。

```
# id username
```

ここで、*username* は、外部グループメンバーの名前です。Satellite では、外部グループを設定する前に、少なくとも 1 人の外部ユーザーが初めて認証する必要があります。また、外部認証ソースには少なくとも 1 人のユーザーが存在する必要があります。

手順8.6 外部ユーザーグループの設定:

1. **Administer (管理) → User Groups (ユーザーグループ)** に移動します。**New User Group (新規ユーザーグループ)** をクリックします。
2. **User group (ユーザーグループ)** タブで、新規ユーザーグループの名前を指定します。ユーザーは、外部ユーザーグループの更新時に自動的に追加されるため、選択しないでください。
3. **Roles (ロール)** タブで、ユーザーグループに割り当てるロールを選択します。または、**Administrator (管理者)** チェックボックスを選択して利用可能なすべてのパーミッションを割り当てます。
4. **External groups (外部グループ)** タブで **Add external user group (外部ユーザーグループの追加)** をクリックし、**Auth source (認証ソース)** ドロップダウンメニューから認証ソースを選択します。

   Name (名前) フィールドに LDAP または外部グループの名前を指定します。
5. **送信** をクリックします。

重要

ユーザーログイン時に自動的にユーザーグループメンバーシップを同期するために LDAP ソースを設定できます。このオプションが設定されていない場合、LDAP ユーザーグループは、LDAP 認証ソースを (デフォルトでは 30 分ごとに) 同期するスケジュールされたタスク (cron ジョブ) により自動的に更新されます。LDAP 認証ソースのユーザーグループがスケジュールされたタスクの間の時間に変更された場合、ユーザーは間違った外部ユーザーグループに割り当てられる可能性があります。この問題は、スケジュールされたタスクが実行されたときに自動的に修正されます。また、**foreman-rake ldap:refresh_usergroups** を実行したり、Web UI で外部ユーザーグループを更新したりすることにより LDAP ソースを手動で更新することもできます。

IdM または AD に基づいた外部ユーザーグループは、グループメンバーが Satellite にログインした場合のみ更新されます。Satellite GUI で外部ユーザーグループのユーザーメンバーシップを変更することはできません。このような変更はグループの次回更新時に上書きされます。外部ユーザーに追加パーミッションを割り当てるには、外部マッピングが指定されていない内部ユーザーグループにそのユーザーを追加します。次に、必要なロールをそのグループに割り当てます。

8.5. プロビジョンされたホストの外部認証

本項では、プロビジョニングされたホストを認証するために IdM 統合を設定する方法について説明します。最初に Satellite または Capsule Server で IdM レルムサポートを設定し、次にホストを IdM レルムグループに追加します。

8.5.1. Red Hat Satellite Server または Capsule Server での IdM レルムサポートの設定

プロビジョニングされたホストに対して IdM を使用するには、最初に Red Hat Satellite Server または Red Hat Satellite Capsule Server を設定します。

前提条件

- Satellite Server がコンテンツ配信ネットワークに登録されているか、または独立した Capsule Server が Satellite Server に登録されています。
- Red Hat Identity Management などのレルムまたはドメインプロバイダーが設定されています。

手順8.7 Red Hat Satellite Server または Capsule Server での IdM レルムサポートの設定:

1. Satellite Server または Capsule Server に以下のパッケージをインストールします。

```
# yum install ipa-client foreman-proxy ipa-admintools
```

2. IdM クライアントとして Satellite Server (または Capsule Server) を設定します。

```
# ipa-client-install
```

3. Satellite Server または Capsule Server の Red Hat Identity Management で realm-capsule ユーザーと関連ロールを作成します。

```
# foreman-prepare-realm admin realm-capsule
```

foreman-prepare-realm を実行して、Capsule Server と使用するよう IdM サーバーを準備します。これにより、Satellite に必要なパーミッションを持つ専用ロールと、そのロールを持つユーザーが作成され、keytab ファイルが取得されます。この手順では Identity Management サーバー設定の詳細が必要になります。

コマンドが正常に実行されると、以下のコマンド出力が表示されるはずです。

```
Keytab successfully retrieved and stored in: freeipa.keytab
Realm Proxy User:    realm-capsule
Realm Proxy Keytab:  /root/freeipa.keytab
```

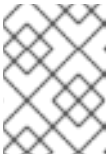
4. **/root/freeipa.keytab** を **/etc/foreman-proxy** ディレクトリーに移し、ユーザーの foreman-proxy に所有者設定を行います。

```
# mv /root/freeipa.keytab /etc/foreman-proxy
# chown foreman-proxy:foreman-proxy /etc/foreman-
proxy/freeipa.keytab
```

5. Satellite Server または Capsule Server のどちらを使用しているかに応じてレルムを設定します。

   - Satellite Server で統合された Capsule Server を使用している場合は、レルムを設定するために **satellite-installer** を使用します。

```
# satellite-installer --foreman-proxy-realm true \
--foreman-proxy-realm-keytab /etc/foreman-proxy/freeipa.keytab \
--foreman-proxy-realm-principal 'realm-capsule@EXAMPLE.COM' \
--foreman-proxy-realm-provider freeipa
```



注記

これらのオプションは、Red Hat Satellite Server を初めて設定する場合にも実行できます。

   - 独立した Capsule Server を使用している場合は、レルムを設定するために **satellite-installer --scenario-capsule** を使用します。

```
# satellite-installer --scenario-capsule --realm true \
--realm-keytab /etc/foreman-proxy/freeipa.keytab \
--realm-principal 'realm-capsule@EXAMPLE.COM' \
--realm-provider freeipa
```

6. ca-certificates パッケージの最新バージョンがインストールされ、IdM 認証局が信頼されていることを確認します。

```
# cp /etc/ipa/ca.crt /etc/pki/ca-trust/source/anchors/ipa.crt
# update-ca-trust enable
# update-ca-trust
```

7. (オプション) すでに存在する Satellite Server または Capsule Server で IdM を設定している場合は、設定の変更を反映するために以下の手順も実行する必要があります。

   a. foreman-proxy サービスを再起動します。

```
# service foreman-proxy restart
```

b. Satellite Server にログインし、**インフラストラクチャー → Capsule** をクリックします。

c. IdM 用に設定した Capsule Server の右側にあるドロップダウンメニューをクリックし、**Refresh Features (機能の更新)** を選択します。

8. 最後に、Satellite Server ユーザーインターフェースで新規のレルムエントリーを作成します。

a. **インフラストラクチャー → レルム** をクリックしてから、メインページの右側にある **新規レルム** をクリックします。

b. 以下のサブタブにフィールドに入力します。

1. **Realm (レルム)** サブタブで、レルム名、使用するレルムの種類、およびレルムプロキシーを指定します。

2. **Locations (ロケーション)** サブタブで、新規レルムを使用する予定のロケーションを選択します。

3. **Organizations (組織)** サブタブで、新規レルムを使用する予定の組織を選択します。

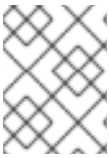
c. **送信** をクリックします。

Satellite Server または Capsule Server は、IdM に自動的に登録されるホストをプロビジョニングできるようになりました。次の項では、ホストを IdM ホストグループに自動的に追加する手順について詳しく説明します。

8.5.2. IdM ホストグループへのホストの追加

Red Hat Enterprise Linux Identity Management (IdM) では、システムの属性に基づいて自動メンバーシップルールをセットアップできます。Red Hat Satellite のレルム機能は、管理者に対し、Red Hat Satellite ホストグループを IdM パラメーター「userclass」にマップする機能を提供します。これにより、管理者は automembership を設定することができます。

ネスト化されたホストグループが使用される場合、それらは Red Hat Satellite ユーザーインターフェースに表示され、IdM サーバーに送信されます。たとえば、"Parent/Child/Child" のように表示されます。



注記

Satellite Server または Capsule Server はアップデートを IdM サーバーに送信しますが、automembership のルールは、初期登録時にのみ適用されます。

手順8.8 IdM ホストグループへのホストの追加:

1. IdM サーバー上で、ホストグループを作成します。

```
# ipa hostgroup-add hostgroup_name
Description: hostgroup_description
----------------------------
Added hostgroup "hostgroup_name"
```

```
----------------------------
Host-group: hostgroup_name
Description: hostgroup_description
```

ここで、

1. *hostgroup_name* はホストグループの名前です。
2. *hostgroup_description* はホストグループの説明です。

2. automembership のルールを作成します。

```
# ipa automember-add --type=hostgroup automember_rule
----------------------------------
Added automember rule "automember_rule"
----------------------------------
Automember Rule: automember_rule
```

ここで、

1. ***automember-add*** は automember グループとしてグループにフラグを立てます。
2. ***--type=hostgroup*** は、ターゲットグループがユーザーグループではなく、ホストグループであることを特定します。
3. *automember_rule* は、automember ルールの特定に使用する名前です。

3. userclass 属性に基づいて automembership の条件を定義します。

```
# ipa automember-add-condition --key=userclass --type=hostgroup --
inclusive-regex=^webserver hostgroup_name
----------------------------------
Added condition(s) to "hostgroup_name"
----------------------------------
Automember Rule: automember_rule
Inclusive Regex: userclass=^webserver
----------------------------
Number of conditions added 1
----------------------------
```

ここで、

1. ***automember-add-condition*** により、グループメンバーを特定するための正規表現の条件を追加することができます。
2. ***--key=userclass*** はキー属性を userclass に指定します。
3. ***--type=hostgroup*** は、ターゲットグループがユーザーグループではなく、ホストグループであることを特定します。
4. ***--inclusive-regex=***^*webserver* は、一致する値を特定するための正規表現パターンです。
5. *hostgroup_name* はターゲットホストグループの名前です。

システムが Satellite Server の *hostgroup_name* ホストグループに追加されると、そのシステムは、

Identity Management サーバーの "*hostgroup_name*" ホストグループにも自動的に追加されます。IdM ホストグループは、HBAC (ホストベースアクセス制御)、sudo ポリシー、およびその他の IdM 機能を許可します。

---

[4] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/linux-manual.html

[5] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/host-attr.html

[6] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/services.h

[7] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/configurir host-access.html

[8] https://access.redhat.com/solutions/67895

[9] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/active-directory-trust.html

[10] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/sssd-gpo.html

第9章 SATELLITE SERVER のカスタマイズ

Red Hat Satellite Server は、ユーザーインターフェースプラグインの追加と、オーケストレーションおよび Rails イベントによりトリガーされたフックの使用で拡張できます。一部のプラグインはデフォルトでインストールされますが、追加のプラグインは Red Hat リポジトリーとアップストリームから RPM パッケージとしてインストールできます。Red Hat は、その API をサポートしますが、アップストリームプラグイン自体はサポートしません。一部のフックは RPM パッケージとして提供され、シェルスクリプトとして作成できるフックもあります。これにより、シェルスクリプトの知識がある管理者は、Ruby と Rails を使用せずに Satellite の機能を拡張することが可能になります。

9.1. プラグインの追加

設定されたリポジトリーから利用可能なプラグインをリストするには、**root** で以下のコマンドを入力します。

```
# yum search rubygem-foreman
Loaded plugins: product-id, search-disabled-repos, subscription-manager
================== N/S matched: rubygem-foreman
==============================
tfm-rubygem-foreman-redhat_access.noarch : Foreman engine to access Red
Hat knowledge base and manage support cases.
tfm-rubygem-foreman-tasks.noarch : Tasks support for Foreman with Dynflow
integration
tfm-rubygem-foreman_abrt.noarch : Display reports from Automatic Bug
Reporting Tool in Foreman
tfm-rubygem-foreman_bootdisk.noarch : Create boot disks to provision hosts
with Foreman出力省略
```

現在インストールされているプラグインを表示するには、**root** で以下のコマンドを入力します。

```
# yum list installed | grep rubygem-foreman
```

新しいプラグインを追加するには、パッケージをインストールし、Foreman を再起動します。たとえば、SCAP クライアントプラグインをインストールするには、**root** で以下のコマンドを入力します。

```
# yum install rubygem-foreman_scap_client.noarch
```

プラグインを登録するために Foreman サービスを再起動します。

```
# touch ~foreman/tmp/restart.txt
```

Foreman Web サイトには追加のプラグイン Popular Plugins[11] があります。Red Hat はプラグイン API をサポートしますが、アップストリームプラグイン自体はサポートしないことに注意してください。

Foreman リポジトリーからのプラグインの追加

Foreman リポジトリーは、yum.theforeman.org/plugins で利用可能です。各 Foreman リリースには、その特定のバージョンと互換性があるプラグインを含む独立したリポジトリーが利用可能です。Foreman のバージョンと互換性があるプラグインをシステムにインストールします。使用している Foreman のリリースを調べるには、以下のコマンドを入力します。

```
$ rpm -q foreman
foreman-1.7.2.53-1.el7sat.noarch
```

以下のように Foreman リポジトリーを設定します。

```
# /etc/yum.repos.d/foreman-plugins.repo
[foreman-plugins]
name=Foreman plugins
baseurl=http://yum.theforeman.org/plugins/1.10/el/x86_64/
enabled=1
gpgcheck=0
```

ここで、*X* は、それぞれ Red Hat Enterprise Linux 6 または 7 向けの**6** または **7** です。使用中の Foreman のリリースに合わせて URL のバージョン番号を変更します。パッケージは現在 GPG 署名されていないことに注意してください。

1. 検索機能を使用してプラグインのパッケージを見つけます。たとえば、名前に "discovery" という単語があるプラグインを検索するには、以下のコマンドを実行します。

   ```
   # yum search discovery
   ```

   または、プラグインの名前のプラグインドキュメンテーションを確認します。

2. たとえば、以下のようにパッケージをインストールします。

   ```
   # yum install tfm-rubygem-foreman_discovery
   ```

3. プラグインを登録するために Foreman サービスを再起動します。

   ```
   # touch ~foreman/tmp/restart.txt
   ```

9.2. FOREMAN フックの使用

Foreman のホストオーケストレーションは、追加のタスクを実行できるようフックで拡張できます。Foreman フックを使用すると、ホストの作成時やホストのプロビジョニングの完了時などのオーケストレーションイベントが発生するときに、スクリプトをトリガーできます (どのような実行可能ファイルでも使用できます)。また、フックはスクリプトとともに Foreman オブジェクトの標準的な Rails コールバックに組み込むことができます。

注記

Foreman フックは Satellite のワークフローを変更できるため、Red Hat からサポートを得るためにすべてのフックを削除するよう求められることがあります。また、Foreman フックはアップグレードの前に削除し、Satellite が期待どおり動作していることを確認した後に復元する必要があります。

Foreman フックは、デフォルトでインストールされる tfm-rubygem-foreman_hooks パッケージにより提供されます。必要な場合は、パッケージがインストールされ、最新の状態であることを確認するために、**root** で以下のコマンドを入力します。

```
# yum install tfm-rubygem-foreman_hooks
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Package tfm-rubygem-foreman_hooks-0.3.9-2.el7sat.noarch already installed
and latest version
Nothing to do
```

Foreman フックは **/usr/share/foreman/config/hooks/** に格納されます。各 Foreman オブジェクトには 1 つのサブディレクトリーを作成する必要があります (各イベント名には他のサブディレクトリーが作成されます)。Foreman オブジェクトは、ホストまたはネットワークインターフェースである場合があります。フックへのパスは以下のようになります。

```
/usr/share/foreman/config/hooks/object/event/hook_script
```

たとえば、ホストでオペレーティングシステムのインストールが完了した後にフックをアクティベートするためにサブディレクトリーを作成するには、以下のようにコマンドを入力します。

```
# mkdir -p /usr/share/foreman/config/hooks/host/managed/before_provision/
```

スクリプトをダウンロードし、適切な名前が指定されたディレクトリーがすでに作成されている場合は、以下のように **install** コマンドを使用して SELinux コンテキストが正しいことを確認します。

```
install hook_script
/usr/share/foreman/config/hooks/object/event/hook_script
```

または、イベントサブディレクトリーに直接スクリプトを作成した場合は、**root** で以下のコマンドを入力して SELinux コンテキストを適用します。

```
# restorecon -RvF /usr/share/foreman/config/hooks
```

SELinux コンテキストは Red Hat Enterprise Linux 6 の場合は **bin_t**、Red Hat Enterprise Linux 7 の場合は **foreman_hook_t** です。スクリプトは制限のある状態で実行されるため、一部のアクションが SELinux によって拒否される場合があることに注意してください。SELinux により拒否されたアクションを確認するには、**aureport -a** を実行するか、**/var/log/audit/audit.log** を調べます。

SELinux の問題のデバッグと **audit2allow** ユーティリティーの使用の詳細については、以下のトピックを参照してください。

- Red Hat Enterprise Linux 6 の場合は、Fixing Problems[12] を参照してください。
- Red Hat Enterprise Linux 7 の場合は、Fixing Problems[13] を参照してください。

手順9.1 Foreman フックを作成してロガーコマンドを使用

このフックスクリプトは、Foreman が新しいサーバーをプロビジョニングするたびに追加のログメッセージを作成します。

1. Satellite Server ベースシステムでディレクトリー構造を作成します。

```
# mkdir -p
/usr/share/foreman/config/hooks/host/managed/before_provision/
```

2. 以下のようにスクリプトを作成します。

```
# vi
/usr/share/foreman/config/hooks/host/managed/before_provision/10_log
ger.sh
#!/bin/bash/
logger $1 $2
```

ファイル名 **_logger.sh** の前の数値からなる接頭辞 *10* により、同じサブディレクトリー内のスクリプトの実行順序が決定します。ニーズに合わせてこの接頭辞を変更します。

3. スクリプトの所有者を **foreman** に変更します。

```
# chown foreman:foreman 10_logger.sh
```

4. ユーザーによる実行を許可するためにスクリプトのパーミッションを変更します。

```
# chmod u+x 10_logger.sh
```

5. SELinux コンテキストが **/usr/share/foreman/config/hooks** ディレクトリー内のすべてのファイルで正しいことを確認します。

```
# restorecon -RvF /usr/share/foreman/config/hooks/
```

6. **foreman** ユーザーが **logger** コマンドを使用できるようにするために、以下のルールを **/etc/sudoers** ファイルに追加します。

```
# vi /etc/sudoers
foreman ALL=(ALL) NOPASSWD:/usr/bin/logger
```

7. フックを登録するために Foreman サービスを再起動します。

```
# touch ~foreman/tmp/restart.txt
```

各 Foreman または Rail オブジェクトにはフックを含めることができます。**/usr/share/app/models/** ディレクトリーを確認するか、利用可能なモデルの完全なリストを取得するために、以下のコマンドを入力します。

```
# foreman-rake console
>
ActiveRecord::Base.descendants.collect(&:name).collect(&:underscore).sort
=> ["audited/adapters/active_record/audit", "compute_resource",
"container",出力省略
```

このコマンド出力は、Foreman フックで使用されない可能性が高いいくつかの技術的な表 ("active_record" や "habtm" など) もリストします。最も一般的に使用されるものは以下のとおりです。

- host
- レポート

9.2.1. オーケストレーションイベント

Foreman は、オブジェクトが作成、更新、および破棄されたときに、ホストおよびネットワークインターフェース (オブジェクトと呼ばれます) 向けのオーケストレーションタスクをサポートします。これらのタスクは Web UI でユーザーに表示されます。タスクが失敗した場合は、アクションのロールバックが自動的にトリガーされます。オーケストレーションフックには優先度を割り当てることができるため、組み込みオーケストレーション手順の前または後 (たとえば、DNS レコードがデプロイされる前) にオーケストレーションフックを呼び出すことができます。

フックをイベントに追加するには、以下のイベント名を使用します。

- create
- update
- destroy

9.2.2. Rails イベント

(上述したオーケストレーションをサポートする) ホストと NIC 以外のものに対するフックの場合は、標準的な Rails イベントを使用できます。各イベントには "before" フックと "after" フックがあります。提供される最も興味深いイベントは以下のとおりです。

- after_create
- before_create
- after_destroy
- before_destroy

ホストオブジェクトでは、以下の 2 つの追加コールバックを使用できます。

- **host/managed/after_build** は、ホストがビルドモードに切り替わったときにトリガーされます。
- **host/managed/before_provision** は、ホストで OS のインストールが完了したときにトリガーされます。

Rails イベントの完全なリストについては、*Ruby on Rails* ActiveRecord::Callbacks[14] ドキュメンテーションの項「Constants」を参照してください。

9.2.3. フックの実行

フックは Foreman サーバーのコンテキスト (したがって、通常は **foreman** ユーザー下) で実行されます。最初の引数は常にイベント名であり、スクリプトを複数のイベントディレクトリーにシンボリックリンクすることを可能にします。2 つ目の引数はフックされたオブジェクトの文字列表現 (たとえば、ホストのホスト名) です。

```
~foreman/config/hooks/host/managed/create/50_register_system.sh create
foo.example.com
```

フックオブジェクトの JSON 表現は標準入力で渡されます。この JSON は v2 API ビューによって生成されます。**jgrep** でこれを読み取るユーティリティーは **examples/hook_functions.sh** で提供され、ほとんどのユーザーにとっては、このユーティリティースクリプトを source コマンドで実行するだけで十分です。それ以外の場合は、パイプバッファーがいっぱいになり、Foreman スレッドがブロックされることを防ぐために、標準入力を閉じることが推奨されます。

```
echo '{"host":{"name":"foo.example.com"}}' \
  | ~foreman/config/hooks/host/managed/create/50_register_system.sh \
       create foo.example.com
```

イベントディレクトリー内の各フックは、アルファベット順に実行されます。オーケストレーションフックの場合は、フックのファイル名の整数接頭辞が優先度値として使用されます。このため、DNS、DHCP、VM 作成、および他のタスクに関連して実行するタイミングが影響を受けます。

9.2.4. フックの失敗とロールバック

フックが失敗し、ゼロ以外のリターンコードで終了した場合は、イベントがログに記録されます。Rails イベントの場合は、他のフックの実行が続行されます。オーケストレーションイベントの場合は、失敗によってアクションが中止され、ロールバックが実行されます。別のオーケストレーションアクションが失敗した場合は、そのアクションをロールバックするためにフックが再び呼び出されることがあります。この場合は、最初の引数が適切に変更されるため、スクリプトで処理する必要があります (たとえば、"create" フックは、あとでロールバックする必要がある場合、"destroy" とともに呼び出されます)。

---

[11] http://projects.theforeman.org/projects/foreman/wiki/List_of_Plugins

[12] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Troubleshooting-Fixing_Problems.html

[13] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/sect-Security-Enhanced_Linux-Troubleshooting-Fixing_Problems.html

[14] http://api.rubyonrails.org/classes/ActiveRecord/Callbacks.html