Red Hat Satellite 6.4

Red Hat Satellite の管理

Red Hat Satellite の管理ガイド

Last Updated: 2018-12-20

Red Hat Satellite 6.4 Red Hat Satellite の管理

Red Hat Satellite の管理ガイド

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

法律上の通知

概要

本ガイドでは、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 を正常にインストールしておく必要があります。

目次

第1章 RED HAT SATELLITE へのアクセス **6**
1.1. RED HAT SATELLITE へのログイン 6
1.2. パスワードの変更 8
1.3. 管理ユーザーパスワードのリセット 8
1.4. ログインページでのカスタムメッセージの設定 9

第2章 RED HAT SATELLITE の起動および停止 **10**

第3章 外部データベースへの移行 **11**
3.1. 外部データベースとして MONGODB を使用する際の注意点 11
3.2. 外部データベースとして POSTGRESQL を使用する際の注意点 12
3.3. 概要 12
3.4. MONGODB のインストール 13
3.5. POSTGRESQL のインストール 14

第4章 ANSIBLE ロールの管理 **17**
4.1. ANSIBLE ロールのインポート 17
4.2. RED HAT ENTERPRISE LINUX システムロールの追加 17

第5章 ユーザーとロールの管理 **19**
5.1. ユーザー管理 19
5.1.1. ユーザーの作成 19
5.1.2. ユーザーへのロールの割り当て 20
5.1.3. SSH キー 20
5.1.4. ユーザーの SSH キー管理 20
5.1.5. E メール通知 21
5.1.6. E メール通知の設定 22
5.1.7. E メールの配信テスト 22
5.1.8. E メール通知のテスト 23
5.1.9. 通知タイプ 23
5.2. ユーザーグループの作成と管理 23
5.2.1. ユーザーグループ 23
5.2.2. ユーザーグループの作成 24
5.2.3. ユーザーグループの削除 24
5.3. ロールの作成および管理 24
5.3.1. ロールの作成 24
5.3.2. ロールのクローン作成 25
5.3.3. ロールへのパーミッションの追加 25
5.3.4. ロールのパーミションの表示 26
5.3.5. パーミッションの完全テーブルの作成 26
5.3.6. ロールの削除 27
5.3.7. ユーザーロールの例 27
5.3.8. Satellite で利用可能な事前定義済みロール 29
5.4. 詳細なパーミッションフィルタリング 31
5.4.1. 詳細なパーミッションフィルター 31
5.4.2. 詳細なパーミッションフィルターの作成 31
5.4.3. 詳細なパーミッションフィルターの使用例 32
5.4.3.1. ホストリソースタイプのパーミッションの適用 32
5.4.3.2. 組織固有のマネージャーロールの作成 32
5.4.4. 詳細な検索に対してサポートされる演算子 33

第6章 セキュリティーコンプライアンスの管理 **35**
6.1. セキュリティーコンテンツの自動化プロトコル 35

6.1.1. SCAP コンテンツ 35
6.1.2. XCCDF プロファイル 35
6.1.2.1. 利用可能な XCCDF プロファイルの一覧表示 35
6.2. SCAP コンテンツの設定 36
6.2.1. OpenSCAP Puppet モジュールのインポート 36
6.2.2. デフォルト OpenSCAP コンテンツのロード 36
6.2.3. 追加の SCAP コンテンツ 36
6.2.3.1. 追加の SCAP コンテンツのアップロード 36
6.3. コンプライアンスポリシーの管理 37
6.3.1. コンプライアンスポリシー 37
6.3.2. ポリシーの作成 37
6.3.3. ポリシーの表示 38
6.3.4. ポリシーの編集 38
6.3.5. ポリシーの定義 38
6.3.6. ホストへのポリシーの追加 38
6.4. テーラリングファイル 39
6.4.1. テーラリングファイルのアップロード 39
6.4.2. テーラリングファイルのポリシーへの割り当て 39
6.5. コンプライアンスのモニター 40
6.5.1. コンプライアンスポリシーダッシュボード 40
6.5.2. コンプライアンスレポートの概要 41
6.5.3. コンプライアンスレポートの検索 41
6.5.4. コンプライアンスレポートの表示 42
6.5.4.1. Evaluation Characteristics (評価特性) 42
6.5.4.2. Compliance and Scoring (コンプライアンスおよびスコアリング) 43
6.5.4.3. Rule Overview (ルールの概要) 43
6.5.4.4. ルール結果の検査 43
6.5.5. コンプライアンスのメール通知 44
6.6. OPENSCAP でサポートされる仕様 44

第7章 SATELLITE SERVER および CAPSULE SERVER のバックアップ 45
7.1. SATELLITE SERVER および CAPSULE SERVER のバックアップ 45
7.1.1. バックアップサイズの予測 45
7.1.2. Satellite Server および Capsule Server の完全バックアップの実行 47
7.1.3. Pulp コンテンツなしでのバックアップの実行 48
7.1.4. 増分バックアップの実行 48
7.1.5. 例 - 週次の完全バックアップの後に日次増分バックアップを実行する 49
7.1.6. オンラインバックアップの実行 50
7.1.7. スナップショットバックアップの実行 51
7.1.8. ホワイトリスト化とステップの省略 51

第8章 バックアップからの SATELLITE SERVER または CAPSULE SERVER の復元 53
8.1. 仮想マシンのスナップショットを使用した CAPSULE SERVER のバックアップと復元 54

第9章 SATELLITE SERVER および CAPSULE SERVER の名前変更 56
9.1. SATELLITE SERVER の名前変更 56
9.2. CAPSULE SERVER の名前変更 58

第10章 SATELLITE SERVER のメンテナンス 61
10.1. 監査レコードの削除 61
10.2. 監査レコードの匿名化 61
10.3. 未使用タスクのクリーニング 61
10.4. 完全なディスクからのリカバリー 62
10.5. MONGODB からのディスク領域の確保 63

10.6. SATELLITE SERVER での RED HAT INSIGHTS の使用 63

第11章 問題のログとレポート 65
11.1. ログとレポート機能 65
11.2. デバッグロギングの有効化 66
11.3. ログファイルからの情報の収集 67
11.4. サポートケースでのログファイルの使用 67
11.5. 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 68
11.5.1. Red Hat Access プラグインでのソリューションの検索 68
11.5.2. Red Hat Access プラグインでのログの使用 69
11.5.3. 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 69
11.5.4. Red Hat Access プラグインを使用した既存サポートケースの編集 70
11.5.5. Red Hat Access プラグインを使用した既存サポートケースの作成 70

第12章 外部認証の設定 72
12.1. LDAP の使用 73
12.1.1. TLS での セキュア LDAP (LDAPS) の設定 73
12.1.2. LDAP を使用するよう Red Hat Satellite を設定する 74
12.1.3. LDAP 設定の説明と例 75
12.1.3.1. LDAP フィルターの例 77
12.2. IDENTITY MANAGEMENT の使用 78
12.2.1. Identity Management の直接的な使用 78
12.2.2. LDAP 認証での Identity Management の使用 80
12.3. ACTIVE DIRECTORY の使用 80
12.3.1. Active Directory の使用 80
12.3.2. フォレスト間信頼での Active Directory の使用 83
12.3.3. LDAP 認証での Active Directory の使用 84
12.4. 外部ユーザーグループの設定 84
12.5. プロビジョンされたホストの外部認証 85
12.5.1. Red Hat Satellite Server または Capsule Server での IdM レルムサポートの設定 85
12.5.2. IdM ホストグループへのホストの追加 87

第13章 SATELLITE SERVER 機能の拡張 90
13.1. SATELLITE プラグイン 90
13.1.1. プラグインの検索 90
13.1.2. プラグインのインストール 91
13.1.3. Foreman リポジトリーの設定 91
13.2. FOREMAN フック 92
13.2.1. Foreman フックのインストール 92
13.2.2. Foreman フックの作成 93
13.2.3. Foreman フックを作成してロガーコマンドを使用 93
13.2.4. オーケストレーションイベント 95
13.2.5. Rails イベント 95
13.2.6. フックの実行 95
13.2.7. フックの失敗とロールバック 96

第14章 リソースのモニタリング 97
14.1. RED HAT SATELLITE コンテンツダッシュボードの使用 97
14.1.1. タスクの管理 100
14.2. RSS 通知の設定 101
14.3. SATELLITE SERVER のモニタリング 101
14.4. CAPSULE SERVER のモニタリング 102
14.4.1. 一般的な Capsule 情報の表示 102
14.4.2. サービスのモニタリング 102

14.4.3. Puppet の監視 103
14.5. トレンドのモニタリング 103

第15章 検索およびブックマーク機能 105
15.1. 検索クエリーの構築 105
15.1.1. クエリーの構文 105
15.1.2. 演算子 105
15.1.3. 値 107
15.2. フリーテキスト検索の使用 107
15.3. ブックマークの管理 108
15.3.1. ブックマークの作成 108
15.3.2. ブックマークの削除 108

付録A SATELLITE の設定 110

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。

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おり、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を通知する警告が表示されることがあります。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://satellite.example.com/pub`** を開きます。
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。

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://satellite.example.com/`

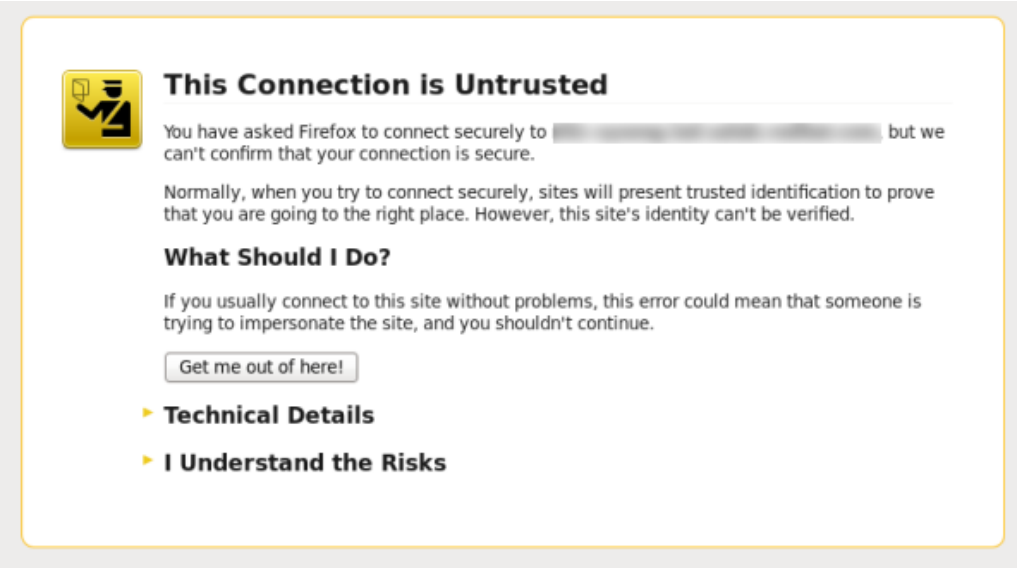
   Satellite Server の完全修飾ドメイン名を確認するには、**`hostname -f`** コマンドを使用します。

   ```
   # hostname -f
   ```

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。



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。デフォルトの管理者アカウント **admin** のパスワードを忘れてしまった場合は、「パスワードの変更」 を参照してください。

ログイン後

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。詳細については、Red Hat Satellite コンテンツのダッシュボードの使用 と 検索およびブックマーク を参照してください。

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
すべてのコンテキスト	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。
Red Hat Access	Red Hat ナレッジベース、Satellite ログファイル、サポートケースへのアクセスを提供します。
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。
	環境に対する重要な変更が管理者に通知されるようにイベントの通知が表示されます。
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。

1.2. パスワードの変更

以下の手順は、パスワードを変更する方法を示しています。

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 **マイアカウント** を選択します。
3. **現在のパスワード** フィールドに現在のパスワードを入力します。
4. **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。
5. **確認** フィールドに新しいパスワードを再入力します。
6. **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。

1.3. 管理ユーザーパスワードのリセット

以下の手順は、管理ユーザーパスワードをリセットする方法を示しています。

管理ユーザーパスワードのリセット

1. Satellite Server がインストールされているマシンにログインします。
2. 以下のコマンドを実行してパスワードをリセットします。
   -

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

3. Web インターフェースにログインして、パスワードを変更します。

1.4. ログインページでのカスタムメッセージの設定

ログインページにカスタムメッセージを設定するには、以下の手順を実行します。

1. **管理** > **設定** に移動して、**全般** タブをクリックします。
2. **ログインページフッターテキスト** の横にある編集ボタンをクリックして、ログインページに表示させるテキストを入力します。たとえば、自社で必須とされる警告メッセージなどにすることができます。
3. **保存** をクリックします。
4. Satellite の web UI からログアウトして、ログインページで Satellite バージョン番号の下にカスタムテキストが表示されることを確認します。

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 **foreman-maintain service** コマンドを提供します。このコマンドは Satellite のバックアップを作成する場合に役に立ちます。バックアップ作成に関する詳細は、「Satellite Server および Capsule Server のバックアップ」 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後に、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。

```
# foreman-maintain service list
```

実行中のサービスのステータスを確認するには、以下のコマンドを実行します。

```
# foreman-maintain service status
```

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

```
# foreman-maintain service stop
```

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

```
# foreman-maintain service start
```

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

```
# foreman-maintain service restart
```

第3章 外部データベースへの移行

Red Hat Satellite のインストールプロセスの一部として、**satellite-installer** コマンドは MongoDB および PostgreSQL のデータベースを Satellite と同じサーバー上にインストールします。Satellite のデプロイメントによっては、外部データベースがサーバーの負荷を軽減する場合もあります。お使いの Satellite デプロイメントが外部データベースを必要とする場合は、内部データベースをこの外部データベースに移行することが可能です。

外部データベースに MongoDB と PostgreSQL のどちらのデータベースが使用できるかについては、要件によって異なります。

Red Hat では、外部データベースのメンテナンスのサポートやそのためのツールは提供していません。これにはバックアップ、アップグレード、データベースのチューニングが含まれます。外部データベースを使用しているお客様は、外部データベースをサポート、メンテナンスする独自のデータベース管理者が必要になります。

お使いの Satellite Server のデータベースが内部のものか、それとも外部のものかを判断するには、データベースのステータスをクエリします。たとえば、以下のコマンドに **--only** と **postgresql** または **rh-mongodb34-mongod** を追加して実行します。

PostgreSQL の場合は、以下のコマンドを実行します。

```
# foreman-maintain service status --only postgresql
```

MongoDB の場合は、以下のコマンドを実行します。

```
# foreman-maintain service status --only rh-mongodb34-mongod
```

お使いの Satellite デプロイメントで外部データベースを必要とする場合は、以下の情報を使用して、Satellite から外部データベースにポイントするように設定します。

3.1. 外部データベースとして MONGODB を使用する際の注意点

Pulp は MongoDB データベースを使用します。MongoDB を外部データベースとして使用する場合は、以下の情報を参照してお使いの Satellite 設定にこのオプションが適しているかどうかを判定してください。

外部 MongoDB の利点

- Satellite 上の空きメモリーと空き CPU が増えます。
- Satellite 操作にマイナスの影響をもたらすことなく MongoDB サーバーのシステムを調整する柔軟性が得られます。

外部 MongoDB のマイナス点

- デプロイメントの複雑性が増し、問題解決がより困難になります。
- 外部 MongoDB サーバーだと、パッチおよびメンテナンス対象に新たなシステムが加わることになります。
- Satellite または Mongo データベースサーバーのいずれかにハードウェアまたはストレージ障害が発生すると、Satellite が機能しなくなります。

- Satellite と外部データベースサーバーの間でレイテンシーが発生すると、パフォーマンスに影響が出ます。

お使いの Mongo データベースが遅いと感じられる場合は、Red Hat サポートチームと協力して問題解決に当たることができます。Satellite 6 での設定問題や既存のパフォーマンス問題については、外部データベースサーバーに移行したとしても解決が期待できないものもあります。Red Hat サポートチームは既知の問題を調査するほか、Satellite エンジニアリングチームとも協力して根本原因を見つけ出します。

3.2. 外部データベースとして POSTGRESQL を使用する際の注意点

Foreman、Katello、および Candlepin は PostgreSQL データベースを使用します。PostgreSQL を外部データベースとして使用する場合は、以下の情報を参照してお使いの Satellite 設定にこのオプションが適しているかどうかを判定してください。

外部 PostgreSQL の利点

- Satellite 上の空きメモリーと空き CPU が増えます。
- PostgreSQL データベースで **`shared_buffers`** を高い値に設定しても、Satellite 上の他のサービスの妨げるリスクがありません。
- Satellite 操作にマイナスの影響をもたらすことなく PostgreSQL サーバーのシステムを調整する柔軟性が得られます。

外部 PostgreSQL のマイナス点

- デプロイメントの複雑性が増し、問題解決がより困難になります。
- 外部 PostgreSQL サーバーだと、パッチおよびメンテナンス対象に新たなシステムが加わることになります。
- Satellite または PostgreSQL データベースサーバーのいずれかにハードウェアまたはストレージ障害が発生すると、Satellite が機能しなくなります。
- Satellite と外部データベースサーバーの間でレイテンシーが発生すると、パフォーマンスに影響が出ます。

お使いの Satellite 上の PostgreSQL データベースがパフォーマンスを低下させていることが疑われる場合は、 Satellite 6: How to enable postgres query logging to detect slow running queries を参照して遅いクエリがあるかどうか判定します。1 秒以上かかるクエリがある場合は、通常、大規模インストールのパフォーマンスが原因であることが多く、外部データベースに移行しても問題解決が期待できません。遅いクエリがある場合は、Red Hat サポートチームまでお問い合わせください。

3.3. 概要

Satellite 用に外部データベースを作成、使用するには、以下の手順を実行します。

1. **『オンラインネットワークからの SATELLITE SERVER のインストール』**のストレージの要件とガイドライン を参照して、外部データベースのストレージ要件をプラニングします。。
2. PostgreSQL で Foreman および Candlepin 用のデータベースを準備し、Foreman と Candlepin のそれぞれのユーザーに対して所有者ロールを用意します。
3. **`pulp_database`** を所有している Pulp ユーザーで MongoDB を準備します。

4. 既存の Satellite データベースのバックアップを作成します。

5. 内部 Satellite データベースを外部データベースに移行します。

6. **satellite-installer** コマンドの引数を編集して新規データベースをポイントするようにし、**satellite-installer** を実行します。

Red Hat Enterprise Linux Server 7 をデータベースインストール用に準備する

必要となるのは最新の Red Hat Enterprise Linux Server 7 でプロビジョニングされた新たなシステムで、これは『**オンラインネットワークからの SATELLITE SERVER のインストール**』の ストレージの要件とガイドライン に記載されているストレージ要件を満たしている必要があります。

1. Satellite サブスクリプションをお使いのサーバーに割り当てます。詳細については、『**オンラインネットワークからの SATELLITE SERVER のインストール**』の Satellite サブスクリプションの確認、およびホストへのサブスクリプションの割り当て を参照してください。

2. MongoDB および PostgreSQL サーバーを Red Hat Enterprise Linux Server 7 にインストールするには、すべてのリポジトリーを無効にし、以下のリポジトリーのみを有効にする必要があります。

```
# subscription-manager repos --disable "*"
# subscription-manager repos --enable=rhel-server-rhscl-7-rpms \
--enable=rhel-7-server-rpms
```

3.4. MONGODB のインストール

インストール可能な MongoDB は、内部データベースのインストール中に **satellite-installer** ツールでインストールされたものと同じバージョンの MongoDB のみになります。MongoDB はサポート対象のバージョンであれば、Red Hat Software Collections (RHSCL) リポジトリーからまたは外部ソースからインストールすることが可能です。Satellite は MongoDB バージョン 3.4 をサポートしています。

1. MongoDB をインストールするには、以下のコマンドを入力します。

```
# yum install rh-mongodb34
```

2. **rh-mongodb34-mongod** サービスを起動して有効にします。

```
# systemctl start rh-mongodb34-mongod
# systemctl enable rh-mongodb34-mongod
```

3. MongoDB で Pulp ユーザーを作成します。

```
# mongo admin -u admin -p admin_password --eval
"db.createUser({user:'pulp',pwd:'Pulp_Password',roles:
[{role:'dbOwner', db:'pulp_database'},{ role: 'readWrite', db:
'pulp_database'}]})"
```

4. **/etc/opt/rh/rh-mongodb34/mongod.conf** ファイルを編集して **security** セクションの認証を有効にします。

```
security:
  authorization: enabled
```

5. **/etc/opt/rh/rh-mongodb34/mongod.conf** ファイルでバインド IP を指定します。

```
bindIp: your_mongodb_server_bind_IP,::1
```

6. **rh-mongodb34-mongod** サービスを再起動します。

```
# systemctl restart rh-mongodb34-mongod
```

7. MongoDB にポート 27017 を開きます。

```
# firewall-cmd --add-port=27017/tcp
# firewall-cmd --add-port=27017/tcp --permanent
```

8. Satellite Server から新規の MongoDB にアクセスできるかどうかテストします。

```
# scl enable rh-mongodb34 "mongo --host mongo.example.com -u pulp -p
Pulp_Password --port 27017 --eval 'ping:1' pulp_database"
```

3.5. POSTGRESQL のインストール

インストール可能な PostgreSQL は、内部データベースのインストール中に **satellite-installer** ツールでインストールされたものと同じバージョンの PostgreSQL のみになります。Satellite がサポートするのは、Red Hat Enterprise Linux Server 7 リポジトリーから入手可能な特定バージョンの PostgreSQL のみになります。PostgreSQL はサポート対象のバージョンであれば、Red Hat Enterprise Linux Server 7 リポジトリーからまたは外部ソースからインストールすることが可能です。サポート対象の PostgreSQL バージョンを格納しているリポジトリーについての情報は、Package Manifest を参照してください。

1. PostgreSQL をインストールするには、以下のコマンドを入力します。

```
# yum install postgresql-server
```

PostgreSQL を初期化して起動、有効にするには、以下のコマンドを実行します。

```
# postgresql-setup initdb
# systemctl start postgresql
# systemctl enable postgresql
```

2. **/var/lib/pgsql/data/postgresql.conf** ファイルを編集します。

```
# vi /var/lib/pgsql/data/postgresql.conf
```

3. 以下の行から # を削除して、着信接続をリッスンするようにします。

```
listen_addresses = "*"
```

4. **/var/lib/pgsql/data/pg_hba.conf** ファイルを編集します。

```
# vi /var/lib/pgsql/data/pg_hba.conf
```

5. 以下の行を追加します。

-

```
  host  all   all   satellite_server_ip/24   md5
```

6. **postgreSQL** サービスを再起動して、変更を適用します。

```
# systemctl restart postgresql
```

7. **postgres** ユーザーに切り替え、PostgreSQL クライアントを起動します。

```
$ su - postgres -c psql
```

8. Foreman と Candlepin 用にそれぞれ、ユーザー、データベース、および専用ロールを作成します。

```
CREATE USER "foreman" WITH PASSWORD 'Foreman_Password';
CREATE USER "candlepin" WITH PASSWORD 'Candlepin_Password';
CREATE DATABASE foreman OWNER foreman;
CREATE DATABASE candlepin OWNER candlepin;
```

9. 外部 PostgreSQL サーバーで **postgresql** ポートを開きます。

```
# firewall-cmd --add-service=postgresql
# firewall-cmd --add-service=postgresql --permanent
```

10. Satellite Server からデータベースにアクセスできるかどうかテストします。

```
# PGPASSWORD='Foreman_Password' psql -h postgres.example.com  -p
5432 -U foreman -d foreman -c "SELECT 1 as ping"
# PGPASSWORD='Candlepin_Password' psql -h postgres.example.com -p
5432 -U candlepin -d candlepin -c "SELECT 1 as ping"
```

外部データベースへの移行

内部データベースを外部データベースに移行するには、以下の手順に従います。

1. Satellite Server で Satellite サービスを停止します。

```
# foreman-maintain service stop
```

2. **postgreSQL** および **mongod** のサービスを起動します。

```
# systemctl start postgresql
# systemctl start mongod
```

3. 内部データベースのバックアップを作成します。

```
# foreman-maintain backup online --skip-pulp-content --preserve-
directory -y /var/migration_backup
```

4. データを新規外部データベースに転送します。

```
PGPASSWORD='Satellite_Password' pg_restore -h postgres.example.com -
U foreman -d foreman < /var/migration_backup/foreman.dump
PGPASSWORD='Candlepin_Password' pg_restore -h postgres.example.com -
```

```
U candlepin -d candlepin < /var/migration_backup/candlepin.dump
mongorestore --host mongo.example.com --db pulp_database --username
pulp --password Pulp_Password /var/migration_backup/mongo_dump
```

5. **satellite-installer** コマンドを使って Satellite が新規データベースをポイントするように更新します。

```
satellite-installer --scenario satellite \
    --foreman-db-host postgres.example.com \
    --foreman-db-password Foreman_Password \
    --foreman-db-database foreman \
    --foreman-db-manage false \
    --katello-candlepin-db-host postgres.example.com \
    --katello-candlepin-db-name candlepin \
    --katello-candlepin-db-password Candlepin_Password \
    --katello-candlepin-manage-db false \
    --katello-pulp-db-username pulp \
    --katello-pulp-db-password Pulp_Password \
    --katello-pulp-db-seeds mongo.example.com:27017 \
    --katello-pulp-db-name pulp_database \
    --katello-pulp-manage-db false
```

第4章 ANSIBLE ロールの管理

Satellite では、Ansible ロールと Red Hat Enterprise Linux システムのロールをインポートして、ルーティンタスクの自動化に役立てることができます。デフォルトでは Ansible は Satellite と Capsule 上で有効になっています。

カスタムまたはサードパーティーの Ansible ロールを使用する場合は、使用することになる Capsule または Satellite の **/etc/ansible/roles** ディレクトリーにそのロールを追加する必要があります。

Satellite 内における Ansible のサポートレベルについての詳細は、**リリースノート** の 新機能および改良された機能 セクションで **Satellite での Ansible のサポート** を参照してください。

Ansible ロールは使用前に **/etc/ansible/roles** ディレクトリーから Satellite Server にインポートする必要があります。

4.1. ANSIBLE ロールのインポート

Ansible ロールは、Ansible が有効になっている Capsule か、Satellite Server がインストールされている **/etc/ansible/roles** ディレクトリーからインポートできます。

Ansible ロールをインポートするには、以下の手順を実行します。

1. Satellite Web UI で、**設定** > **ロール** に移動して、インポートするロールが含まれている Capsule をクリックします。
2. Ansible ロール一覧からインポートするロールのチェックボックスを選択し、**更新** をクリックします。

4.2. RED HAT ENTERPRISE LINUX システムロールの追加

Red Hat Enterprise Linux システムロールは Red Hat Enterprise Linux 7.4 でテクニカルプレビューとして導入されたもので、Red Hat Enterprise Linux サブシステムの設定インターフェイスです。Red Hat Enterprise Linux システムロールを利用すると Satellite 内の Ansible ロールを追加することができます。Satellite の Ansible ロールを使用すると、設定がより速くかつ容易に実行できます。

Red Hat Enterprise Linux システムロールについての詳細は、Red Hat Enterprise Linux System Roles を参照してください。

Optional および Supplementary チャンネルをサブスクライブする前に、対象範囲の詳細 を参照してください。

Red Hat Enterprise Linux システムロールの追加方法:

1. **rhel-7-server-extras-rpms** リポジトリーが有効になっていることを確認します。

```
# subscription-manager repos --enable=rhel-7-server-extras-rpms
```

2. **rhel-system-roles** パッケージをインストールします。

```
# yum install rhel-system-roles
```

rhel-system-roles パッケージは **/usr/share/ansible/roles/** にダウンロードされます。インポート前に修正を加えることができます。

3. **rhel-7-server-extras-rpms** リポジトリーを無効にします。

```
# subscription-manager repos --disable=rhel-7-server-extras-rpms
```

4. Satellite Web UI で、**設定** > **ロール** に移動して、インポートするロールが含まれている Capsule をクリックします。

5. Ansible ロール一覧からインポートするロールのチェックボックスを選択し、**更新** をクリックします。

これで Ansible ロールをホストまたはホストグループに割り当てることができます。詳細については、**ホストの管理** の 既存ホストへの Ansible ロールの割り当て を参照してください。

また、Ansible のジョブテンプレートに追加すると、ロール内に含まれているモジュールを Ansible playbooks に追加することもできます。ジョブテンプレートには **hosts:all** 行を含める必要があります。詳細については、Red Hat Enterprise Linux (RHEL) System Roles を参照してください。

第5章 ユーザーとロールの管理

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、ユーザーグループでまとめ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と管理」 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。

5.1. ユーザー管理

管理者は、Satellite ユーザーを作成、変更、および削除できます。また、異なる **ロール** をユーザーやユーザーのグループに割り当てることで、アクセスパーミッションを設定することもできます。

5.1.1. ユーザーの作成

Satellite Web UI を使ってユーザーを作成します。

手順

1. **管理** > **ユーザー** に移動します。
2. **ユーザーの作成** をクリックします。
3. **ログイン** フィールドにユーザーのユーザー名を入力します。
4. **名** および **姓** フィールドに、ユーザーの本当の姓名を入力します。
5. **Email アドレス** フィールドに email アドレスを入力します。
6. **説明** フィールドには、新規ユーザーの説明を加えます。
7. **言語** 一覧からユーザー用の言語を選択します。
8. **タイムゾーン** 一覧からタイムゾーンを選択します。
   デフォルトでは、Satellite Server はユーザーのブラウザーの言語とタイムゾーンを使用します。
9. ユーザーのパスワードを設定します。
   a. **認証先** 一覧から、ユーザー認証に使用するソースを選択します。
      - **内部**: Satellite Server 内でのユーザー管理を有効にします。
      - **LDAP または IdM**: 12章*外部認証の設定* の説明にある外部認証を設定します。

b. **パスワード** フィールドに初期パスワードを入力して、**確認** フィールドで再入力します。

10. **送信** をクリックしてユーザーを作成します。

5.1.2. ユーザーへのロールの割り当て

Satellite web UI を使用してユーザーにロールを割り当てます。

手順

1. **管理** > **ユーザー** に移動します。
2. ロールを割り当てるユーザーの **ユーザー名** をクリックします。

注記

ユーザーアカウントが表示されない場合は、現在適切な組織を表示しているかどうかを確認します。Satellite の全ユーザーを一覧表示するには、**デフォルトの組織** をクリックしてから **任意の組織** をクリックします。

3. **ロケーション** タブをクリックして、ロケーションが割り当てられていない場合は選択します。
4. **組織** タブをクリックして、組織が割り当てられていることを確認します。
5. **ロール** タブをクリックして利用可能なロールのリストを表示します。
6. **ロール** リストから割り当てるロールを選択します。
   利用可能な全パーミッションを付与するには、**管理** チェックボックスを選択します。
7. **送信** 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、**ロール** タブをクリックします。割り当てられたロールは、**選択された項目** に表示されます。割り当てたロールを削除するには、**選択された項目** でロール名をクリックします。

5.1.3. SSH キー

ユーザーに SSH キーを追加すると、プロビジョニング中に SSH キーのデプロイメントが可能になります。

プロビジョニング中に SSH キーをデプロイする方法については、『**プロビジョニングガイド**』 の プロビジョニング中の SSH キーのデプロイ を参照してください。

SSH キーおよびその作成方法についての詳細は、『Red Hat Enterprise Linux 7 システム管理者のガイド』の 鍵ベース認証の使用 を参照してください。

5.1.4. ユーザーの SSH キー管理

Satellite web UI からユーザーの SSH キーを追加または削除します。

注記

Red Hat Satellite 管理ユーザーとして Web UI にログインするか、SSH キーの追加には **create_ssh_key** パーミッションを有効にしたユーザーとして、キーの削除には **destroy_ssh_key** パーミッションを有効にしたユーザーとしてログインしてください。

手順

1. **管理** > **ユーザー** に移動します。
2. **ユーザー名** コラムから必要となるユーザーのユーザー名をクリックします。
3. **SSH キー** タブをクリックします。
   - SSH キーの追加
     i. 公開 SSH キーのコンテンツをクリップボードに用意します。
     ii. **SSH キーの追加** をクリックします。
     iii. **キー** フィールドに公開 SSH キーのコンテンツをクリップボードから貼り付けます。
     iv. **名前** フィールドに SSH キーの名前を入力します。
     v. **送信** をクリックします。
   - SSH キーの削除
     i. 削除する SSH キーの列にある **削除** をクリックします。
     ii. 確認メッセージで **OK** をクリックします。

5.1.5. E メール通知

E メール通知は Satellite Server が定期的に作成するか、特定イベントの完了後に作成されます。定期通知は、毎日、毎週、または毎月のいずれかに送信することができます。

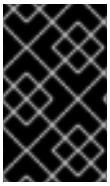
通知をトリガーするイベントは以下のとおりです。

- ホストのビルド
- コンテンツビューのプロモーション
- ホストが報告するエラー
- リポジトリーの同期

デフォルトでは、ユーザーには E メールは通知されません。通知のタイプや頻度などの基準に基づいて、ユーザーが通知を受信するように管理者が設定できます。

注記

E メール通知を個人の E メールアドレスではなくグループの E メールアドレスに送信する場合は、グループの E 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。



重要

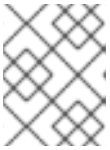
Satellite Server は、デフォルトでは送信メールを有効にしないため、E メール設定を確認する必要があります。詳細は『**オンラインネットワークからの SATELLITE SERVER のインストール**』の Satellite Server での送信メールの設定 を参照してください。

5.1.6. E メール通知の設定

Satellite Web UI で E メール通知を設定します。

手順

1. **管理** > **ユーザー** に移動します。
2. 編集する **ユーザー名** をクリックします。
3. **ユーザー** タブで、**メール** フィールドの値を確認します。E メールは、このフィールドのアドレスに送信されます。
4. **電子メール設定** タブで **メールの有効化** を選択します。
5. 通知タイプの横にあるドロップダウンメニューから、ユーザーが受信する通知を選択します。



注記

メールクエリー テキストボックスに必要なクエリを記入すると、**Audit Summary** 通知をフィルターすることができます。

6. **送信** をクリックします。
通知メールのユーザーへの送信が開始されます。

5.1.7. E メールの配信テスト

E メールの配信を確認するには、テストメールをユーザーに送信します。メールが配信されれば、設定が適切であることを確認できます。

手順

1. Satellite Web UI で、**管理** > **ユーザー** に移動します。
2. ユーザー名をクリックします。
3. **E メール設定** タブで **テスト E メール** をクリックします。
ユーザーの E メールアドレスにすぐにテストメッセージが送信されます。

E メールが配信されれば、確認は完了です。配信されない場合は、以下の診断ステップを実行してください。

a. ユーザーのメールアドレスを確認します。
b. Satellite Server のメール設定を確認します。
c. ファイアウォールおよびメールサーバーのログを調べます。

5.1.8. E メール通知のテスト

ユーザーが正常に E メール通知をサブスクライブしていることを確認するには、手動で通知をトリガーします。

手順

- 通知をトリガーするには、以下のコマンドを実行します。

```
# foreman-rake reports:<frequency>
```

frequency を以下のいずれかで置き換えます。

  - daily (毎日)
  - weekly (毎週)
  - monthly (毎月)

これでサブスクライブしている全ユーザーに指定された頻度ですべての予定されている通知が配信されます。全ユーザーが通知を受信すれば、確認ができたことになります。

注記

手動でトリガーした通知を個別ユーザーに送信することは、現在サポートされていません。

5.1.9. 通知タイプ

Satellite では以下の通知が作成されます。

- **監査サマリー**: Satellite Server が監査した全アクティビティーのサマリー。
- **ホストの構築**: ホストが構築されるとこの通知が送信されます。
- **ホストエラータアドバイザリー**: 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。
- **OpenSCAP ポリシーサマリー**: OpenSCAP ポリシーレポートとその結果の概要。
- **エラータのプロモート**: 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。これにより、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。
- **Puppet エラー状態** : ホストが Puppet に関連するエラーを報告した後に送信される通知です。
- **Puppet サマリー** : Puppet レポートのサマリーです。
- **エラータの同期** : 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。

5.2. ユーザーグループの作成と管理

5.2.1. ユーザーグループ

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集合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ピングできます。

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。

5.2.2. ユーザーグループの作成

Satellite Web UI を使ってユーザーグループを作成します。

手順

1. **管理** > **ユーザーグループ** に移動します。
2. **ユーザーグループの作成** をクリックします。
3. **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、グループメンバーを選択します。
   - **ユーザーグループ** のリストから、以前に作成したユーザーグループを選択します。
   - **ユーザー** のリストからユーザーを選択します。
4. **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、**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. **送信** をクリックします。

5.2.3. ユーザーグループの削除

Satellite Web UI を使ってユーザーグループを削除します。

手順

1. **管理** > **ユーザーグループ** に移動します。
2. 削除するユーザーグループの右側にある **削除** 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グループを削除します。

5.3. 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となる事前定義済みロール一式が提供されます (「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。

5.3.1. ロールの作成

Satellite Web UI を使ってロールを作成します。

手順

1. **管理** > **ロール** に移動します。
2. **ロールの作成** をクリックします。
3. ロールの **名前** を記入します。
4. **送信** をクリックして、新しいロールを保存します。

ロールにはパーミッションを含める必要があります。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。

5.3.2. ロールのクローン作成

Satellite Web UI を使ってロールのクローンを作成します。

手順

1. **管理** > **ロール** に移動して、必要なロールの右側にあるドロップダウンメニューから **クローン** を選択します。
2. ロールの **名前** を記入します。
3. **送信** をクリックしてロールのクローンを作成します。
4. クローンされたロールの名前をクリックし、**フィルター** に移動します。
5. 必要に応じて、パーミッションを編集します。
6. **送信** をクリックして、新しいロールを保存します。

5.3.3. ロールへのパーミッションの追加

Satellite Web UI を使ってパーミッションをロールに追加します。

手順

1. **管理** > **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 **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 **リソースタイプ** を選択します。**(その他)** 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 **パーミッション** リストからクリックします。
5. **リソースタイプ** での選択により、**無制限** と **上書き** のチェックボックスが表示されます。**無制限** チェックボックスはデフォルトで選択され、選択されたタイプの全リソースにパーミッションが適用されます。**無制限** チェックボックスを無効にすると、**検索** フィールドが有効になり、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。**上書き** チェックボックスを有効にすると、新たなロケーションと組織を追加して、それらのロケーションや組織のリソースタイプにこのロールがアクセスできるようになります。また、既に関連付けられたロケーションや組織をリソースタイプから削除して、アクセスを制限することもできます。

6. **次へ** をクリックします。

7. **送信** をクリックして変更を保存します。

5.3.4. ロールのパーミションの表示

Satellite Web UI を使ってロールのパーミッションを表示します。

手順

1. **管理** > **ロール** に移動します。

2. ロールの右側にある **フィルター** をクリックして、**フィルター** ページを開きます。

フィルター ページでは、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示されます。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、「パーミッションの完全テーブルの作成」 を参照してください。

5.3.5. パーミッションの完全テーブルの作成

Satellite Web CLI を使ってパーミッションテーブルを作成します。

手順

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 の最後に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、表を確認します。

5.3.6. ロールの削除

Satellite Web UI を使ってロールを削除します。

手順

1. **管理** > **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 **削除** を選択します。
3. 警告ボックスで、**OK** をクリックしてロールを削除します。

5.3.7. ユーザーロールの例

Satellite 管理者

管理システムおよびアプリケーションを含む、Satellite 全アイテムのアクセス制御がある最上位レベルの管理者ロールです。

IT オペレーションマネージャー

Satellite アイテムの表示パーミッションがある、読み取り専用ロールです。

ライセンス管理所有者

組織およびレポートの表示パーミッションを含む、マニフェストとサブスクリプション管理のパーミッションがあるタスク特定のロールです。

品質保証

専用のテスト環境でテストを実行する環境およびロケーション固有のロールですが、その環境外のアイテムへのアクセスは限定されます。

表5.1 ユーザーロール設定の例

ロール	リソースタイプ	パーミッション	フィルター
Satellite 管理者	**管理者** チェックボックスが選択されていることを確認してください。詳細は、「ユーザーへのロールの割り当て」 を参照してください。	事前設定のパーミッション	
IT オペレーションマネージャー	Viewer	事前設定のパーミッション	

ロール	リソースタイプ	パーミッション	フィルター
ライセンス管理所有者	その他	**access_dashboard my_organizations view_statistics**	
	製品とリポジトリー	**view_products**	
	サブスクリプション	**view_subscriptions attach_subscriptions unattach_subscriptions import_manifest delete_manifest**	
	組織	**view_organizations**	
	レポート	**view_reports**	
	ホスト	**view_hosts**	
品質保証	組織	**view_organizations**	
	環境	**view_environments create_environments edit_environments destroy_environments import_environments**	
	その他	**view_tasks view_statistics access_dashboard**	
	ホストクラス	**edit_classes**	
	ホストグループ	**view_hostgroups edit_hostgroups**	

ロール	リソースタイプ	パーミッション	フィルター
	ホスト	**view_hosts** **create_hosts** **edit_hosts** **destroy_hosts** **build_hosts** **power_hosts** **console_hosts** **ipmi_boot_hosts** **puppetrun_hosts**	
	ロケーション	**view_locations**	
	Puppet クラス	**view_puppetclasses**	
	Capsule	**view_smart_proxies** **view_smart_proxies_autosign** **view_smart_proxies_puppetca**	
	その他	**my_organizations**	
	製品とリポジトリー	**view_products**	
	ホストクラス	**edit_classes**	
	ライフサイクル環境	**view_lifecycle_environments** **edit_lifecycle_environments** **promote_or_remove_content_views_to_environments**	name ~ **QA**
	コンテンツビュー	**view_content_views** **create_content_views** **edit_content_views** **publish_content_views** **promote_or_remove_content_views**	name ~ **ccv***

5.3.8. Satellite で利用可能な事前定義済みロール

ロール	ロールで提供されるパーミッション[a]
Access Insights Admin	Insights のルールの追加、編集。
Access Insights Viewer	Insight レポートの表示。
Bookmarks manager	ブックマークの作成、編集、および削除。
Boot disk access	起動ディスクのダウンロード。
Compliance manager	SCAP コンテンツファイル、コンプライアンスポリシー、テーラリングファイルの表示、作成、編集、破棄。コンプライアンスレポートの表示。
Compliance viewer	コンプライアンスレポートの表示。
Create ARF report	コンプライアンスレポートの作成。
Default role	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。
Edit hosts	ホストを表示、作成、編集、破棄、および構築します。
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。
Manager	管理者のロールに似ているが、グローバル設定の編集パーミッションがありません。Satellite web UI では、グローバル設定は、**管理** > **設定** にあります。
Organization admin	組織ごとに定義された管理者ロール。このロールでは、他の組織のリソースは表示できません。
Red Hat Access Logs	ログビューアーとログを表示します。
Remote Execution Manager	完全リモート実行パーミッションのあるロール。ジョブテンプレートの編集も含まれます。
Remote Execution User	リモート実行ジョブを実行します。
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。

ロール	ロールで提供されるパーミッション[a]
Tasks reader	Satellite タスクの表示のみが可能なロール。
Viewer	Satellite 構造、ログ、レポート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。
View hosts	ホストの表示のみが可能なロール。
Virt-who Manager	完全な virt-who パーミッションのあるロール。
Virt-who Reporter	virt-who が生成したレポートを Satellite にアップロードできます。virt-who を手動で設定して、限定的な virt-who パーミッションを持つユーザーロールが必要な場合に使用できます。
Virt-who Viewer	virt-who 設定の表示ができます。このロールでは、既存の virt-who 設定 を使用した virt-who インスタンスのデプロイができます。

[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、「ロールのパーミションの表示」 で確認できます。

5.4. 詳細なパーミッションフィルタリング

5.4.1. 詳細なパーミッションフィルター

「ロールへのパーミッションの追加」 の説明にあるように、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エリであり、ほとんどのリソースタイプでサポートされています。

5.4.2. 詳細なパーミッションフィルターの作成

Satellite Web UI を使用して詳細なフィルターを作成します。

手順

- **フィルターの編集** ページの **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 **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、「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、**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** や **not**、**has** といった論理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。

注記

Satellite では、検索条件はアクション作成には適用されません。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、ユーザーが新しく作成されたロケーションにカスタム名を割り当てることができないわけではありません。

5.4.3. 詳細なパーミッションフィルターの使用例

管理者は、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。以下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、実稼働環境にプッシュされるとそのコンテンツにはアクセスできなくなります。

5.4.3.1. ホストリソースタイプのパーミッションの適用

以下のクエリは、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
```

以下のクエリーは、**XXXX**, **Yyyy**、または **zzzz** の文字列に名前が一致するレコードを返します。

```
name ^ (XXXX, Yyyy, zzzz)
```

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、**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
```

検索 フィールドでより詳細なパーミッションフィルターを使用すると、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っては、**ロケーション** および **組織** タブを提供する **上書き** チェックボックスが、GUI の代わりとなります。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。「組織固有のマネージャーロールの作成」 を参照してください。

5.4.3.2. 組織固有のマネージャーロールの作成

Satellite UI を使って **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。

手順

1. **管理** > **ロール** に移動します。

2. 既存の **Organization admin** ロールをクローンします。**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 **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 admin**) を挿入するよう求められます。

3. ロールに関連付けるロケーションと組織をクリックします。

4. **送信** をクリックしてロールを作成します。

5. **org-1 admin** をクリックしてから **フィルター** をクリックし、関連付けられたフィルターを確認します。デフォルトのフィルターはほとんどのケースで機能しますが、**編集** をクリックして各フィルターのプロパティーを変更することもできます。フィルターによっては、ロールを追加のロケーションと組織のリソースにアクセス可能としたい場合には、**上書き** オプションを有効にできます。たとえば、**ドメイン** リソースタイプを選択して **上書き** オプションを選択し、**ロケーション** と **組織** タブを使って追加のロケーションと組織を選択すると、このロールに関連付けられていない追加のロケーションと組織のドメインにこのロールがアクセスできるようになります。**新規フィルター** をクリックして、新規フィルターをこのロールに関連付けることもできます。

5.4.4. 詳細な検索に対してサポートされる演算子

表5.2 論理演算子

演算子	説明
and	検索条件を組み合わせます。
not	式を否定します。
has	オブジェクトには指定したプロパティーが必要です。

表5.3 記号演算子

演算子	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。
!=	**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**: 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。これは、**Is equal to** 比較とは別の SQL クエリーを生成し、複数値の値でより効果的なものです。
!^	**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。

第6章 セキュリティーコンプライアンスの管理

セキュリティーコンプライアンス管理は、セキュリティーポリシーの定義、それらのポリシーへのコンプライアンスの監査、およびコンプライアンス違反のインスタンスの解決などを行う継続的なプロセスです。コンプライアンス違反は、組織の設定管理ポリシーに基づいて管理されます。セキュリティーポリシーは、ホスト固有のものから業界共通のものまでに及ぶため、ポリシー定義には柔軟性が必要になります。

6.1. セキュリティーコンテンツの自動化プロトコル

Satellite 6 では、Security Content Automation Protocol (SCAP) を使ってセキュリティー設定ポリシーを定義します。たとえば、セキュリティーポリシーは、Red Hat Enterprise Linux を実行するホストの場合に SSH 経由のログインを **root** アカウントに許可しないように指定することが可能です。Satellite 6 では、管理対象の全ホストについて、コンプライアンスの監査とレポーティングをスケジュールすることができます。SCAP についての詳細は、Red Hat Enterprise Linux 7 セキュリティーガイド を参照してください。

6.1.1. SCAP コンテンツ

SCAP コンテンツは、ホストのチェックに使用される設定およびセキュリティーベースラインが含まれるデータストリーム形式のコンテンツです。チェックリストは extensible checklist configuration description format (XCCDF) および open vulnerability and assessment language (OVAL) の脆弱性に記述されます。ルール とも呼ばれるチェックリスト項目は、システム項目の必要な設定を表します。たとえば、どのユーザーも **root** ユーザーアカウントを使用して SSH 経由でホストにログインできないように指定することができます。ルールは 1 つ以上のプロファイルに分類でき、複数のプロファイルで 1 つのルールを共有できるようにすることができます。SCAP コンテンツはルールとプロファイルの両方で構成されています。

SCAP コンテンツは、作成することも、ベンダーから取得することも可能です。Red Hat Enterprise Linux 用にサポートされるプロファイルは scap-security-guide パッケージで提供されます。SCAP コンテンツの作成については本ガイドで扱いませんが、独自のコンテンツをダウンロードし、デプロイし、変更し、作成する方法についての詳細は、Red Hat Enterprise Linux 7 セキュリティーガイド を参照してください。Red Hat Enterprise Linux と共に提供される SCAP コンテンツは SCAP 仕様 1.2 に準拠しています。

Satellite 6 の OpenSCAP コンポーネントと共に提供されるデフォルトの SCAP コンテンツは、Red Hat Enterprise Linux のバージョンによって異なります。Red Hat Enterprise Linux 7 には、Red Hat Enterprise Linux 6 と Red Hat Enterprise Linux 7 の両方のコンテンツがインストールされます。

6.1.2. XCCDF プロファイル

XCCDF プロファイルは、ホストまたはホストグループの評価に使用されるチェックリストです。プロファイルは、業界標準またはカスタム標準への準拠を確認するために作成されます。

Satellite 6 で提供されるプロファイルは、OpenSCAP project から取得できます。

6.1.2.1. 利用可能な XCCDF プロファイルの一覧表示

Satellite UI で、利用可能な XCCD プロファイルを一覧表示します。

手順

- **ホスト** > **SCAP コンテンツ** に移動します。

6.2. SCAP コンテンツの設定

6.2.1. OpenSCAP Puppet モジュールのインポート

OpenSCAP コンテンツを Puppet 環境にインポートするには、監査する各ホストを Satellite UI で Puppet 環境に関連付ける必要があります。

手順

1. **設定** > **環境** に移動します。
2. **satellite.example.com からの環境のインポート** をクリックします。
3. 監査するホストに関連付けられた Puppet 環境のチェックボックスを選択します。
   Puppet 環境が存在しない場合は、**production** 環境のチェックボックスを選択します。
4. **更新** をクリックします。

6.2.2. デフォルト OpenSCAP コンテンツのロード

CLI で、デフォルトの OpenSCAP コンテンツをロードします。

手順

- 以下のように **foreman-rake** コマンドを使用します。

```
# foreman-rake foreman_openscap:bulk_upload:default
```

6.2.3. 追加の SCAP コンテンツ

追加の SCAP コンテンツは、各自で作成したものか他から取得したものかを問わず、Satellite Server にアップロードできます。SCAP コンテンツは、ポリシーに適用される前に Satellite Server にインポートされる必要があります。たとえば、Red Hat Enterprise Linux 7.2 リポジトリーで利用可能な **scap-security-guide** RPM パッケージには、Payment Card Industry Data Security Standard (PCI-DSS) バージョン 3 向けのプロファイルが含まれます。このコンテンツは、オペレーティングシステムのバージョン固有ではないため、Red Hat Enterprise Linux 7.2 を実行していない場合でも Satellite Server にアップロードできます。

6.2.3.1. 追加の SCAP コンテンツのアップロード

Satellite web UI で追加の SCAP コンテンツをアップロードします。

手順

1. **ホスト** > **SCAP コンテンツ** に移動して、**新規 SCAP コンテンツ** をクリックします。
2. **タイトル** テキストボックスにタイトルを入力します。
   例: **RHEL 7.2 SCAP コンテンツ**.
3. **ファイルの選択** をクリックしてから、SCAP コンテンツファイルが含まれるロケーションに移動し、**開く** を選択します。
4. **送信** をクリックします。

SCAP コンテンツファイルが正常にロードされると、**Successfully created RHEL 7.2 SCAP Content (RHEL 7.2 SCAP コンテンツが正常に作成されました)** といったメッセージが表示され、**SCAP コンテンツ** のリストに新規のタイトルが含まれます。

6.3. コンプライアンスポリシーの管理

6.3.1. コンプライアンスポリシー

コンプライアンスポリシー とも呼ばれる定期監査は、XCCDF プロファイルに対して指定したホストのコンプライアンスをチェックするスケジュールタスクです。スキャンのスケジュールは Satellite Server で指定され、スキャンはホストで実行されます。スキャンが完了すると、**Asset Reporting File** (ARF) が XML 形式で生成され、Satellite Server にアップロードされます。スキャンの結果はコンプライアンスポリシーダッシュボードで確認できます。コンプライアンスポリシーでは、スキャンされるホストに変更はなされません。SCAP コンテンツには、関連付けられたルールのあるいくつかのプロファイルが含まれますが、デフォルトではポリシーは含まれません。

6.3.2. ポリシーの作成

以下の手順に従ってコンプライアンスポリシーを作成します。ここでは 、指定された時間にロケーションおよびホストまたはホストグループのいずれかに適用される SCAP コンテンツとプロファイルを指定します。

前提条件/事前作業

- 「OpenSCAP Puppet モジュールのインポート」

ポリシーを作成するには、以下を実行します。

1. Satellite web UI で、**ホスト** > **ポリシー** に移動して、**新規ポリシー** をクリックしてからウィザードのステップに従います。
2. ポリシーの名前、説明 (オプション) を入力してから **次へ** をクリックします。
3. 適用する SCAP コンテンツおよび XCCDF プロファイルを選択してから **次へ** をクリックします。
4. ポリシーを適用する時間を指定してから **次へ** をクリックします。
   期間 のドロップダウンメニューから、**毎週**、**毎月**、または **カスタム** を選択します。
   - **毎週** を選択したら **平日** ドロップダウンリストから曜日を選択します。
   - **毎月** を選択したら **日付** フィールドで日付を指定します。
   - **カスタム** を選択したら **Cron 行** フィールドに有効な Cron 式を入力します。
     Custom オプションでは、**毎週** もしくは **毎月** オプションよりもスケジュールに柔軟性を持たせることができます。
5. ポリシーを適用するロケーションを選択してから **次へ** をクリックします。
6. ポリシーを適用する組織を選択してから **次へ** をクリックします。
7. ポリシーを適用するホストグループを選択してから **送信** をクリックします。

Puppet エージェントが選択したホストグループに属するホスト、またはポリシーが適用されているホストで実行される場合、OpenSCAP クライアントがインストールされ、Cron ジョブがポリシーの指定

されたスケジュールと共に追加されます。**SCAP コンテンツ** タブでは、すべてのターゲットホストのディレクトリー **/var/lib/openscap/content/** に配信される SCAP コンテンツの名前を指定します。

6.3.3. ポリシーの表示

以下の手順に従って、特定の OpenSCAP コンテンツおよびプロファイルの組み合わせによって適用されるルールのプレビューを行います。これはポリシーを計画する際に便利です。

ポリシーを表示するには、以下を実行します。

1. Satellite web UI で、**ホスト** > **ポリシー** に移動します。
2. **ガイドの表示** をクリックします。

6.3.4. ポリシーの編集

以下の手順に従ってポリシーを編集します。編集されたポリシーは、次に Puppet エージェントが Satellite Server で更新をチェックする際にホストに適用されます。これはデフォルトで 30 分ごとに実行されます。

ポリシーを編集するには、以下を実行します。

1. Satellite web UI で、**ホスト** > **ポリシー** に移動します。
2. ポリシーの名前の右側にあるドロップダウンリストから、**編集** を選択します。
3. 必要な属性を編集します。
4. **送信** をクリックします。

編集されたポリシーは、次に Puppet エージェントが Satellite Server で更新をチェックする際にホストに適用されます。これはデフォルトで 30 分ごとに実行されます。

6.3.5. ポリシーの定義

以下の手順を実行して既存のポリシーを削除します。

1. Satellite web UI で、**ホスト** > **ポリシー** に移動します。
2. ポリシーの名前の右側にあるドロップダウンリストから、**削除** を選択します。
3. 確認メッセージで **OK** をクリックします。

6.3.6. ホストへのポリシーの追加

ホストにポリシーを追加するには、以下の手順に従います。

1. Satellite web UI で、**ホスト** > **すべてのホスト** に移動します。
2. ポリシーを追加するホストを選択します。
3. **アクションの選択** をクリックします。
4. リストから **コンプライアンスポリシーの割り当て** を選択します。

5. 新規パネルで、利用可能なポリシー一覧から適切なポリシーを選択し **送信** をクリックします。

6.4. テーラリングファイル

テーラリングファイルを使うと、既存の OpenSCAP ポリシーを分岐したり書き換えたりせずにカスタマイズすることができます。テーラリングファイルは、ポリシー作成時や更新時にポリシーに割り当てることができます。

テーラリングファイルは SCAP Workbench を使用して作成することができます。SCAP Workbench ツールについての詳細は、Customizing SCAP Security Guide for your use-case を参照してください。

6.4.1. テーラリングファイルのアップロード

Satellite web UI でテーラリングファイルをアップロードします。

手順

1. **ホスト** > **コンプライアンス - テーラリングファイル** に移動して、**新規 テーラリングファイル** をクリックします。
2. **名前** テキストボックスに、名前を入力します。
3. **ファイルの選択** をクリックしてから、SCAP DataStream テーラリングファイルが含まれるロケーションに移動し、**開く** を選択します。
4. **送信** をクリックして、選択したテーラリングファイルをアップロードします。

6.4.2. テーラリングファイルのポリシーへの割り当て

Satellite web UI でテーラリングファイルをポリシーに割り当てます。

手順

1. **ホスト** > **コンプライアンス - ポリシー** に移動します。
2. **新規ポリシー**、または既存のコンプライアンスポリシーがある場合は、**新規コンプライアンスポリシー** をクリックします。
3. **名前** テキストボックスに名前を入力して **次へ** をクリックします。
4. ドロップダウンメニューから **Scap コンテンツ** を選択します。
5. ドロップダウンメニューから **XCCDF プロファイル** を選択します。
6. ドロップダウンメニューから **テーラリングファイル** を選択します。
7. ドロップダウンメニューから **テーラリングファイル内の XCCDF プロファイル** を選択します。テーラリングファイルは複数の XCCDF プロファイルを含めることが可能なため、XCCDF プロファイルの選択が重要になります。
8. **次へ** をクリックします。
9. ドロップダウンメニューから **期間** を選択します。
10. ドロップダウンメニューから **平日** を選択して、**次へ** をクリックします。

11. **選択したアイテム** ウィンドウに移動させる **ロケーション** を選択して、**次へ** をクリックします。

12. **選択したアイテム** ウィンドウに移動させる **組織** を選択して、**次へ** をクリックします。

13. **選択したアイテム** ウィンドウに移動させる **ホストグループ** を選択して、**送信** をクリックします。

6.5. コンプライアンスのモニター

コンプライアンスのモニターは、監査が実行されていることを確認し、コンプライアンス違反を特定するための継続的なタスクです。Red Hat Satellite 6 は一元化したコンプライアンスのモニターと管理を可能にします。Satellite の管理下にあるホストについては、カスタムスケジュールに基づいてコンプライアンス状況のチェックが行われ、詳細が Satellite Server によって照合されます。コンプライアンスダッシュボードでは、ホストのコンプライアンスの概要を示し、ポリシーの範囲内の各ホストの詳細を表示できます。コンプライアンスレポートでは、各ホストの適用可能なポリシーへのコンプライアンスの詳細な分析を行います。この情報を利用して、各ホストが提示するリスクを評価し、ホストのコンプライアンスを確保するために必要なリソースをより効果的に管理できます。

SCAP を使用してコンプライアンスをモニターする際の共通の目的には以下が含まれます。

- ポリシーコンプライアンスの表示
- コンプライアンスの変更の検知

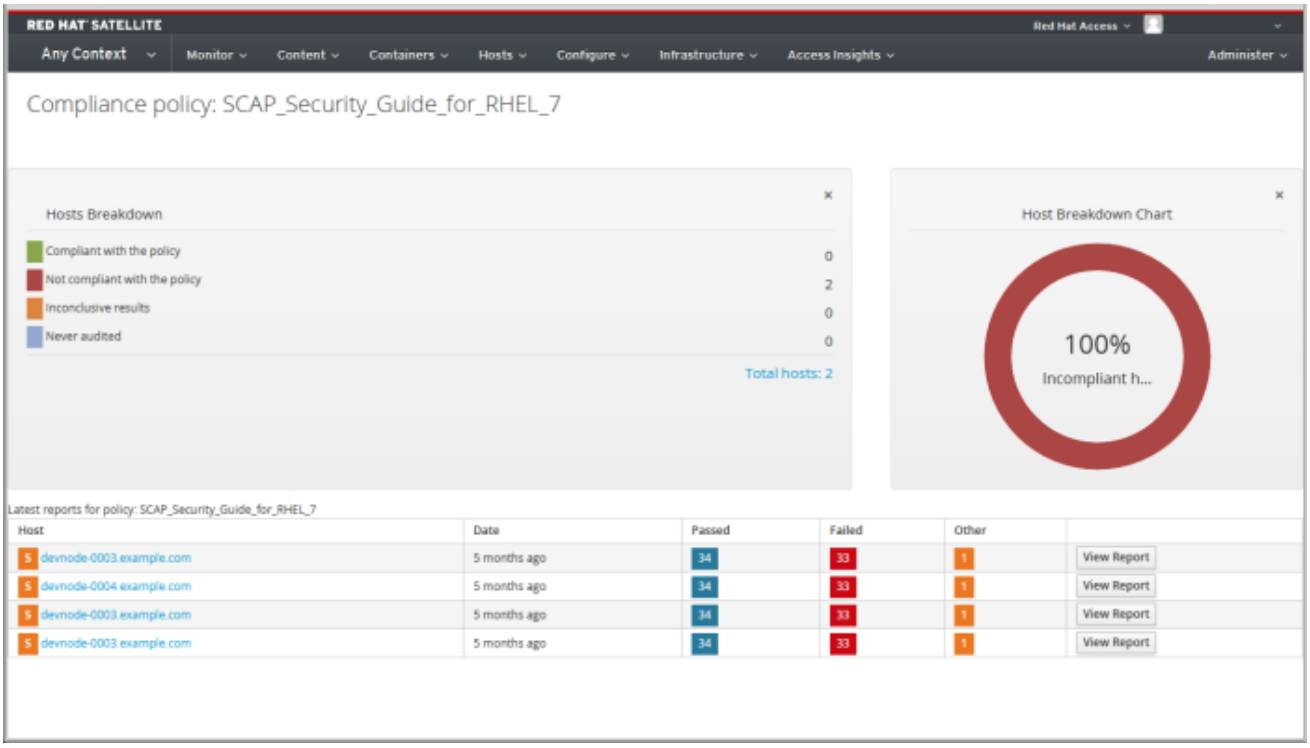
Satellite web UI は、これらの目的を達成するために必要なすべての情報を提供します。コンプライアンスポリシーダッシュボードでポリシーのコンプライアンス状況を検証します。コンプライアンスレポートの履歴を確認するか、または変更のメール通知をサブスクライブするかのいずれかによって、ポリシーコンプライアンスにおける変更を検出します。

6.5.1. コンプライアンスポリシーダッシュボード

コンプライアンスポリシーダッシュボードは、ホストのポリシーへのコンプライアンス状況の概要を示します。コンプライアンスポリシーのダッシュボードを表示するには、Satellite web UI を開いてから **ホスト** > **ポリシー**に移動し、必要なポリシー名をクリックします。ダッシュボードでは以下の情報が提供されます。

- ホストのポリシーへのコンプライアンス状況のハイレベルビューを表示するリングチャート
- ホストのポリシーコンプライアンス状況についての統計の内訳 (表形式)
- 各ホストの最新ポリシーレポートへのリンク

ダッシュボードビューは、ホストのコンプライアンス状況の統計的な概要を表示するため、コンプライアンスの管理をここから開始することができます。コンプライアンス違反として評価されたすべてのホストについては、**`Failed (失敗)`**の統計でコンプライアンスタスクの優先付けに使用できるメトリックを提供します。**未監査** として検出されたホストも、それらの状況が不明なために優先する必要があります。



6.5.2. コンプライアンスレポートの概要

コンプライアンスレポートは、ホストに対して実行されるポリシーの出力です。すべてのコンプライアンスレポートを一覧表示するには、Satellite web UI を開いてから **ホスト** > **レポート** に移動します。各レポートには、ポリシーごとに合格または不合格となったルールの合計数が含まれます。デフォルトでは、レポートは日付の降順で一覧表示されます。並べ替え順序を変更するには、並べ替える列のラベルをクリックします。次に、その同じラベルをもう一度クリックして降順または昇順のいずれかに変更します。個別のレポートを表示するには、**レポートを表示** をクリックします。ホストの全レポート、またはホストのサブセットを表示するには、**検索** フィールドを使用します。コンプライアンスレポートを削除するには、**レポートを表示** の横にある矢印をクリックして、**削除** を選択します。

ホストのポリシーコンプライアンスを管理する際には、一定期間コンプライアンスの変更をモニターすることが役立ちます。**検索** フィールドを使用してレポートの一覧を 1 つ以上のホストに限定し、変更を手動で評価します。または、通知メールを設定することもできます。

6.5.3. コンプライアンスレポートの検索

コンプライアンスレポートの検索フィールドを使用して、ホストのサブセットで入手可能なレポート一覧に範囲を制限します。

フィルターを適用するには、**検索** フィールドに検索条件を入力し、Enter を押すか、または **検索** をクリックします。実行される検索では大文字と小文字が区別されません。

空の **検索** フィールドをクリックすると、利用可能な検索パラメーターが一覧表示されます。

and、**not** および **has** の論理演算子を使用すると複雑なクエリを作成することができます。論理演算子の詳細については、「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。

正規表現は有効な検索基準ではありませんが、単一の検索式に複数のフィールドを使うことが可能です。利用可能な検索演算子については、「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。

検索ユースケース

以下の検索条件では、6 つ以上のルールがパスしなかったコンプライアンスレポートを検索します。

```
failed > 5
```

以下の検索条件では、ホスト名に **prod-** が含まれるホストで、2015 年 11 月 5 日以降に作成されたコンプライアンスレポートが検索されます。

```
host ~ prod- AND date > "Nov 5, 2015"
```

以下の検索条件では、1 時間前より compliance_policy **rhel7_audit** を使用して生成されたすべてのレポートが検索されます。

```
"1 hour ago" AND compliance_policy = date = "1 hour ago" AND
compliance_policy = rhel7_audit
```

すべての 利用可能なコンプライアンスレポートを再び一覧表示するには、**検索** 条件を削除してから、**Enter** を押すか、**検索** をクリックします。

検索条件のブックマーク

検索条件はブックマークすることで、同じ検索条件を再使用することができます。詳細は 「ブックマークの作成」 を参照してください。

ブックマークを使用するには、**ホスト** > **レポート** に移動し、**検索** ボタンの横にあるドロップダウン項目をクリックしてから、ブックマークをクリックします。

6.5.4. コンプライアンスレポートの表示

ホスト > **レポート** に移動して、特定ホストの列にある **レポートの表示** をクリックします。

コンプライアンスレポートは以下のセクションで構成されています。

- はじめに
- Evaluation Characteristics (評価特性)
- Compliance and Scoring (コンプライアンスおよびスコアリング)
- Rule Overview (ルールの概要)

6.5.4.1. Evaluation Characteristics (評価特性)

このセクションでは、評価されたホスト、評価に使用されたプロファイル、および評価の開始と終了を含む、特定のプロファイルに対する評価についての詳細情報を提供します。参照用として ホストの IPv4、IPv6、および MAC アドレスも一覧表示されます。

評価特性

`Target machine`

評価されるホストの完全修飾ドメイン名 (FQDN) です。例: **`test-system.example.com`**

`Benchmark URL`

ホストの評価に使用される SCAP コンテンツの URL です。例: **`/var/lib/openscap/content/1fbdc87d24db51ca184419a2b6f`**

Benchmark ID

ホストの評価に使用されるベンチマークの ID です。ベンチマークはプロファイルのセットです。例: **xccdf_org.ssgproject.content_benchmark_RHEL_7**

Profile ID

ホストの評価に使用されるプロファイルの ID です。例: **xccdf_org.ssgproject_content_profile_rht-ccp**

Started at

ISO 8601 形式で示される評価が開始された日時です。例: **2015-09-12T14:40:02**

Finished at

ISO 8601 形式で示される評価の終了日時です。例: **2015-09-12T14:40:05**

Performed by

評価をホストに実行したローカルのアカウント名です。例: **root**

6.5.4.2. Compliance and Scoring (コンプライアンスおよびスコアリング)

このセクションでは、ホストがプロファイルのルールに準拠しているかどうかの概要、重大度別の非コンプライアンスの内訳、およびパーセンテージで示される全体のコンプライアンススコアを示します。ルールへのコンプライアンスがチェックされなかった場合には、**ルール結果** で **その他**として分類されます。

6.5.4.3. Rule Overview (ルールの概要)

このセクションでは、階層的に示されるルールと共にすべてのルールの詳細とコンプライアンスの結果を示します。

コンプライアンスレポートに組み込まれるルールの一覧を制限するためにチェックボックスを選択したり、クリアしたりします。たとえば、非コンプライアンスを重点的にレビューする場合には、**pass** および **informational** チェックボックスをクリアします。

すべてのルールを検索するには、**検索** フィールドに条件を入力します。検索は、入力時に動的に適用されます。**検索** フィールドは、単一のプレーンテキストの検索用語のみを受け入れ、それは大文字と小文字を区別しない検索に適用されます。検索の実行時には、説明が検索条件に一致するルールのみが一覧表示されます。検索フィルターを削除するには、検索条件を削除します。

各結果の説明については、**結果** コラムに示されるステータスの上にカーソルを移動します。

6.5.4.4. ルール結果の検査

ホストがルールのコンプライアンスに失敗した理由を判別するには、ルールのタイトルをクリックします。次に開かれるウィンドウでは、ルールの説明 (該当する場合は、ホストのコンプライアンスを確保する方法が含まれる)、ルールの根拠、および場合によっては修復スクリプトを含む追加情報が提供されます。

警告

推奨される修復操作やスクリプトのいずれについても、まずそれらを実稼働以外の環境でテストしてから実装するようにしてください。

6.5.5. コンプライアンスのメール通知

Satellite Server は、**Openscap policy summary**(Openscap ポリシー概要) のメール通知をサブスクライブしているすべてのユーザーに、OpenSCAP 概要メールを送信します。通知メールをサブスクライブする方法については、「E メール通知の設定」 を参照してください。ポリシーが実行されるたびに、Satellite は直前の実行との比較で結果をチェックし、変更がないかどうかを確認します。メールは各サブスクライバーがリクエストする頻度で送信され、各ポリシーの概要と直近の結果の概要を提供します。

OpenSCAP の概要 メールメッセージには、以下の情報が含まれます。

- 対象とする期間の詳細。
- すべてのホストの合計 (状況別): 変更済み、準拠、および非準拠。
- 各ホストの表形式の内訳と、合格、失敗、変更済み、または結果が不明な場合などのルールの合計を含む最新ポリシーの結果。

6.6. OPENSCAP でサポートされる仕様

以下の仕様が OpenSCAP でサポートされています。

タイトル	説明	バージョン
XCCDF	Extensible Configuration Checklist Description Format	1.2
OVAL	Open Vulnerability and Assessment Language	5.11
-	Asset Identification	1.1
ARF	Asset Reporting Format	1.1
CCE	Common Configuration Enumeration	5.0
CPE	Common Platform Enumeration	2.3
CVE	Common Vulnerabilities and Exposures	-
CVSS	Common Vulnerability Scoring System	2.0

第7章 SATELLITE SERVER および CAPSULE SERVER のバックアップ

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の継続性を確保するために必要な最小限のバックアップ手順について説明します。デプロイメントでカスタム設定を使用する場合は、バックアップおよび災害復旧ポリシーを策定する際にカスタム設定をどのように扱うかについて考慮する必要があります。

7.1. SATELLITE SERVER および CAPSULE SERVER のバックアップ

本セクションでは、Satellite Server または Capsule Server とすべての関連データのバックアップを **`foreman-maintain backup`** スクリプトで作成する方法について説明します。バックアップは、異なるシステム上の別個のストレージデバイスに作成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くなります。バックアップは、**`cron`** を使用して稼働率が低い時間にスケジュールすることができます。週次の完全バックアップの後に日次増分バックアップを実行する場合を参照してください。

オフラインバックアップまたはスナップショットバックアップ中はサービスが非アクティブになり、Satellite はメンテナンスモードに入ります。ポート 443 上での外部からのトラフィックはすべてファイアウォールで拒否され、修正がトリガーされないようになります。

前提条件

定期的なバックアップを計画する際には、以下の点に注意してください。

- 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、管理者がそれぞれ異なる場所やタイムゾーンで働いている場合に特に重要です。
- バックアップを暗号化するか、安全な場所に移動し、ホストへの不正アクセスや破損のリスクを最小化します。

従来のバックアップ方法

『Red Hat Enterprise Linux 7 システム管理者のガイド』 にある システムバックアップおよびリカバリー セクションで説明されている従来のバックアップ方法を使用することもできます。スナップショットまたは従来のバックアップを作成する際には、すべてのサービスを停止してください (**`foreman-maintain backup`** スクリプトの使用時を除く)。

```
# foreman-maintain service stop
```

スナップショットまたは従来のバックアップを作成したら、サービスを起動します。

```
# foreman-maintain service start
```

7.1.1. バックアップサイズの予測

完全なバックアップでは、MongoDB、PostgreSQL、および Pulp のデータベースファイルと Satellite 設定ファイルの非圧縮アーカイブを作成します。Satellite サービスが利用できない時間を短縮するため、圧縮はアーカイブの作成後に実行されます。その結果、完全なバックアップでは、以下のデータを保存するための領域が必要となります。

- 非圧縮の Satellite データベースおよび設定ファイル。
- 圧縮された Satellite データベースおよび設定ファイル。

- バックアップを確実にするため、予測領域全体の 20% を追加。

バックアップサイズの予測

1. **du** コマンドを入力して、Satellite データベースおよび設定ファイルを含む非圧縮ディレクトリーのサイズを予測します。以下に例を示します。

```
# du -sh /var/lib/mongodb /var/lib/pgsql/data /var/lib/pulp
480G /var/lib/mongodb
100G    /var/lib/pgsql/data
100G /var/lib/pulp
# du -csh /var/lib/qpidd /var/lib/tftpboot /etc /root/ssl-build \
/var/www/html/pub /opt/puppetlabs
886M    /var/lib/qpidd
16M     /var/lib/tftpboot
37M /etc
900K /root/ssl-build
100K /var/www/html/pub
2M /opt/puppetlabs
942M   total
```

2. 圧縮データを保存するために必要な領域を計算します。
表7.1「バックアップデータ圧縮率」 は、バックアップで使用されるすべてのデータアイテムの圧縮率を提示します。

表7.1 バックアップデータ圧縮率

データ型	ディレクトリー	比率	圧縮結果の例
MongoDB データベースファイル	**/var/lib/mongodb**	85 - 90 %	480 GB → 60 GB
PostgreSQL データベースファイル	**/var/lib/pgsql/data**	80 - 85%	100 GB → 20 GB
Pulp RPM ファイル	**/var/lib/pulp**	(非圧縮)	100 GB
設定ファイル	**/var/lib/qpidd** **/var/lib/tftpboot** **/etc** **/root-ssl/build** **/var/www/html/pub** **/opt/puppetlabs**	85%	942 MB → 141 MB

この例では、圧縮されたバックアップデータは合計 180 GB を占有します。

3. バックアップの保存に必要な領域を計算するには、圧縮および非圧縮のバックアップデータの予測値を合計し、合計値の 20% をさらに追加してバックアップの信頼性を高めます。
この例では、非圧縮および圧縮のバックアップデータに 681 GB と 180 GB の合計 861 GB が必要です。172 GB の予備領域もあわせ、1033 GB をバックアップの場所に割り当てる必要があります。

7.1.2. Satellite Server および Capsule Server の完全バックアップの実行

Red Hat Satellite 6.4 では、**foreman-maintain backup** スクリプトを使用してバックアップを作成します。使用方法を表示するには、以下のコマンドを使用します。

```
# foreman-maintain backup --help
```

Satellite Server のバックアップには、以下の 3 つの方法があります。

- オフラインバックアップ
- オンラインバックアップ
- スナップショットバックアップ
  それぞれの方法については、スクリプトごとに以下のコマンドで表示できます。

オフラインバックアップ

```
# foreman-maintain backup offline --help
```

オンラインバックアップ

```
# foreman-maintain backup online --help
```

スナップショットからのバックアップ

```
# foreman-maintain backup snapshot --help
```

ディレクトリーの作成

foreman-maintain 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にタイムスタンプの付いたサブディレクトリーが作成されます。**foreman-maintain backup** スクリプトではバックアップは上書きされないので、バックアップまたは増分バックアップから復元する際には、適切なディレクトリーまたはサブディレクトリーを選択する必要があります。このスクリプトは、必要に応じてサービスを停止したり、再開したりします。

ディレクトリー名を付ける場合は、**--preserve-directory** オプションを追加して名前を追加します。バックアップはコマンドラインで指定したディレクトリーに保存されます。

--preserve-directory を使用すると、バックアップに失敗してもデータは削除されません。

ローカルの PgSQL データベースがある場合は、ユーザー **postgres** はそのディレクトリーへの書き込みアクセスを必要とします。

リモートデータベース

foreman-maintain backup スクリプトを使用してリモートデータベースのバックアップを作成できます。

リモートデータベースのバックアップにはオンラインとオフラインの両方が使用できますが、スナップショットのようなオフライン方法を使用すると **foreman-maintain backup** スクリプトはデータベースダンプを実行します。

Satellite Server または Capsule Server の完全オフラインバックアップの実行

以下の手順では、完全なオフラインバックアップが実行されます。このバックアッププロセス中は、Satellite サービスが利用できなくなります。

警告

Satellite Server および Capsule Server の他のユーザーに、すべての変更を保存するよう指示して、バックアップ中は Satellite サービスが利用できないことを警告してください。バックアップと同じ時間に他のタスクがスケジュールされていないことを確認してください。

1. バックアップの場所に、バックアップを保存するための十分なディスク領域があることを確認します。詳細は 「バックアップサイズの予測」 を参照してください。
2. バックアップスクリプトを実行します。

```
# foreman-maintain backup offline /var/backup_directory
```

コピーするデータサイズのために、このプロセスの完了には時間がかかることがあります。

7.1.3. Pulp コンテンツなしでのバックアップの実行

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。

警告

Satellite Server および Capsule Server の他のユーザーに、すべての変更を保存するよう指示して、バックアップ中は Satellite サービスが利用できないことを警告してください。バックアップと同じ時間に他のタスクがスケジュールされていないことを確認してください。

1. バックアップの場所に、バックアップを保存するための十分なディスク領域があることを確認します。詳細は 「バックアップサイズの予測」 を参照してください。
2. バックアップスクリプトを実行します。

```
# foreman-maintain backup offline --skip-pulp-content
/var/backup_directory
```

7.1.4. 増分バックアップの実行

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、最初の増分バックアップを実行します。少なくとも最後に正常に完了した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。

警告

Satellite Server および Capsule Server の他のユーザーに、すべての変更を保存するよう指示して、バックアップ中は Satellite サービスが利用できないことを警告してください。バックアップと同じ時間に他のタスクがスケジュールされていないことを確認してください。

1. バックアップの場所に、バックアップを保存するための十分なディスク領域があることを確認します。詳細は 「バックアップサイズの予測」 を参照してください。
2. 完全バックアップを作成します。

```
# foreman-maintain backup offline  /var/backup_directory
```

3. **--incremental** 引数を使用してバックアップスクリプトを実行します。これで初回増分バックアップを保存するディレクトリーがバックアップディレクトリー内に作成されます。

```
# foreman-maintain backup offline --incremental
/var/backup_directory/full_backup  /var/backup_directory
```

4. バックアップスクリプトを再度実行して、2 回目の増分バックアップを作成します。次回増分の開始点を示すために、初回増分バックアップをポイントします。これで 2 回目増分バックアップのディレクトリーがバックアップディレクトリー内に作成されます。

```
# foreman-maintain backup offline --incremental
/var/backup_directory/first_incremental_backup
/var/backup_directory
```

別のバージョンのバックアップをポイントし、開始点としてそのバックアップバージョンでの増分シリーズを作成する場合は、いつでもこれを行うことができます。たとえば、初回もしくは 2 回目増分バックアップからではなく、完全バックアップからの増分バックアップを作成するには、完全バックアップディレクトリーをポイントします。

```
# foreman-maintain backup offline --incremental
/var/backup_directory/full_backup  /var/backup_directory
```

7.1.5. 例 - 週次の完全バックアップの後に日次増分バックアップを実行する

週次の完全バックアップの後に日次増分バックアップを実行する場合

以下のスクリプトでは、日曜日に完全バックアップを実行し、その後の他の曜日では増分バックアップを実行します。バックアップが作成される日には、それぞれのサブディレクトリーが作成されます。このスクリプトでは、日次の cron ジョブが必要になります。

```
#!/bin/bash -e
PATH=/sbin:/bin:/usr/sbin:/usr/bin
DESTINATION=/var/backup_directory
if [[ $(date +%w) == 0 ]]; then
  foreman-maintain backup offline --assumeyes $DESTINATION
else
  LAST=$(ls -td -- $DESTINATION/*/ | head -n 1)
  foreman-maintain backup offline --assumeyes --incremental "$LAST"
$DESTINATION
fi
exit 0
```

foreman-maintain backup スクリプトでは、**PATH** 内に **/sbin** ディレクトリーおよび **/usr/sbin** ディレクトリーを格納し、**--assumeyes** オプションが必要になることに注意してください。コマンドではバックアップを進める確認が必要になるためです。

7.1.6. オンラインバックアップの実行

オンラインバックアップはデバッグ目的のみで実行してください。Pulp データベースに影響を与える手順がある場合は、Pulp 部分のバックアップ手順は変更がなくなるまで繰り返されます。Pulp データベースのバックアップは Satellite バックアップの中で最も時間のかかる部分であるため、バックアップ中に Pulp データベースが変更される変更を加えると、バックアップ手順が繰り返されます。

オンラインバックアップに関するリスク

サービスがオンラインの間は、Mongo と Postgres データベース間でデータの不一致が発生する可能性があります。

オンラインバックアップ実行時は、Pulp データベースに影響を与える手順がある場合は、Pulp 部分のバックアップ手順は変更がなくなるまで繰り返されます。Pulp データベースのバックアップは Satellite バックアップの中で最も時間のかかる部分であるため、バックアップ中に Pulp データベースが変更される変更を加えると、バックアップ手順が繰り返されます。

実稼働環境では、スナップショットのバックアップが推奨されます。詳細は 「スナップショットバックアップの実行」 を参照してください。実稼働環境でオンラインバックアップを使用する場合は、バックアップ中に変更がないように注意して実行してください。

警告

Satellite Server および Capsule Server の他のユーザーに、すべての変更を保存するよう指示して、バックアップ中は Satellite サービスが利用できないことを警告してください。バックアップと同じ時間に他のタスクがスケジュールされていないことを確認してください。

オンラインバックアップの実行

1. バックアップの場所に、バックアップを保存するための十分なディスク領域があることを確認します。詳細は 「バックアップサイズの予測」 を参照してください。

2. バックアップスクリプトを実行します。

```
# foreman-maintain backup online /var/backup_directory
```

7.1.7. スナップショットバックアップの実行

スナップショットバックアップでは、Pulp、MongoDB、および PostgreSQL ディレクトリーの論理ボリュームマネージャー (LVM) のスナップショットを使用します。バックアップは、オンラインバックアップの場合と同様に、実行中の Satellite からではなく、LVM スナップショットから作成され、一貫性のないバックアップを作成するリスクを減らします。スナップショットバックアップは完全なオフラインバックアップよりも迅速なので、Satellite のダウンタイムを短縮することができます。

スナップショットバックアップの実行

使用方法を表示するには、以下のコマンドを入力します。

```
foreman-maintain backup snapshot -h
```

前提条件

スナップショットバックアップを開始する前に、以下の条件を満たしていることを確認してください。

- システムがスナップショットするディレクトリーに LVM を使用していること (**/var/lib/pulp/**、**/var/lib/mongodb/**、および **/var/lib/pgsql/**)。
- 関連ボリュームグループ (VG) の空きディスクスペースが、スナップショットのサイズの 3 倍あること。正確には、VG には新規スナップショットを受け入れるために十分な、メンバーの論理ボリューム (LV) に予約されていないスペースが必要になります。また、LV のいずれかには、バックアップディレクトリー用の十分な空きスペースが必要になります。
- ターゲットのバックアップディレクトリーが、スナップショットを作成するディレクトリー以外の LV にあること。

警告

Satellite Server および Capsule Server の他のユーザーに、すべての変更を保存するよう指示して、バックアップ中は Satellite サービスが利用できないことを警告してください。バックアップと同じ時間に他のタスクがスケジュールされていないことを確認してください。

バックアップスクリプトを実行します。

```
# foreman-maintain backup snapshot /var/backup_directory
```

foreman-maintain backup snapshot スクリプトはサービスがアクティブな際にスナップショットを作成し、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を停止します。これにより、メンテナンスの時間が短縮されます。バックアップが正常に実行されると、全サービスが再起動され、LVM スナップショットが削除されます。

7.1.8. ホワイトリスト化とステップの省略

foreman-maintain backup スクリプトを使用したバックアップは、ステップ順に進められます。バックアップの一部を省略するには、**--whitelist** オプションをコマンドに追加し、さらに省略するステップのラベルを追加します。例を示します。

```
# foreman-maintain backup online --whitelist backup-metadata  -y
/var/backup_directory
```

利用可能なステップラベルを一覧表示するには、以下を実行します。

```
# foreman-maintain advanced procedure run -h
```

第8章 バックアップからの SATELLITE SERVER または CAPSULE SERVER の復元

本セクションでは、「Satellite Server および Capsule Server のバックアップ」 の手順で作成されたバックアップデータから Red Hat Satellite Server または Red Hat Capsule Server を復元する方法について説明します。このプロセスでは、バックアップを生成したサーバーと同じサーバーでバックアップが復元され、バックアップでカバーされている全データはターゲットシステム上で削除されます。元のシステムが利用できない場合は、同じ設定およびホスト名でシステムのプロビジョニングを行なってください。

前提条件

- 適切なインスタンスを復元していることを確認します。Red Hat Satellite インスタンスでホスト名、設定が同一であり、メジャーバージョンが元のシステムと同じである必要があります。
- 既存のターゲットディレクトリーがあること。ターゲットディレクトリーは、アーカイブ内に含まれている設定ファイルから読み取られます。ターゲットディレクトリーがない場合は、復元時にエラーが発生します。
- Satellite Server または Capsule Server のベースシステムに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/** 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。
  ディレクトリーのサイズを確認するには、以下のコマンドを入力します。

  ```
  # du -sh /var/backup_directory
  ```

  空き領域のサイズを確認するには、以下のコマンドを入力します。

  ```
  # df -h /var/backup_directory
  ```

  --total オプションを追加すると複数ディレクトリーの合計結果が取得できます。
- **root** で **foreman-maintain restore** スクリプトを実行してください。
- すべての SELinux コンテキストが適切であることを確認します。以下のコマンドを入力して、適切な SELinux コンテキストを復元します。

  ```
  # restorecon -Rnv /
  ```

完全バックアップからの Satellite Server または Capsule Server の復元

1. Satellite 6 のインストールに適した方法を選択します。
   - 接続済みネットワークから Satellite Server をインストールするには、オンラインネットワークからの SATELLITE SERVER のインストール の手順に従います。
   - 非接続ネットワークから Satellite Server をインストールするには、オフラインネットワークからの SATELLITE SERVER のインストール の手順に従います。
   - Capsule Server をインストールするには、CAPSULE SERVER のインストール の手順に従います。
2. バックアップデータを Satellite Server のローカルファイルシステム (**/var/** または **/var/tmp/**) にコピーします。

3. 復元スクリプトを実行します。

```
# foreman-maintain restore /var/backup_directory
```

ここでの **backup_directory** は、バックアップされたデータを格納しているタイムスタンプ付きのディレクトリーまたはサブディレクトリーになります。

コピーするデータサイズのために、この復元プロセスは時間がかかることがあります。増分バックアップがある場合は、増分バックアップからの Satellite Server または Capsule Server の復元 を参照してください。

復元プロセスが完了するとすべてのプロセスがオンラインになり、すべてのデータベースおよびシステム設定がバックアップ時の状態に戻ります。

トラブルシューティングを行うには、**/var/log/foreman/production.log** および **/var/log/messages** にあるファイルを参照してください。

増分バックアップからの Satellite Server または Capsule Server の復元

増分バックアップから Satellite または Capsule Server を復元するには、以下の手順を実行します。複数の増分バックアップのブランチがある場合は、完全バックアップと復元したいブランチの各増分バックアップを時系列で選択します。

1. 8章 *バックアップからの Satellite Server または Capsule Server の復元*の手順に従って、最後の完全バックアップを復元します。
2. **/var/** や **/var/tmp/** などの Satellite Server のローカルファイルシステムから完全バックアップデータを削除します。
3. **/var/** や **/var/tmp/** などの Satellite Server のローカルファイルシステムに増分バックアップデータをコピーします。
4. 増分バックアップが作成された順序で復元します。

```
# foreman-maintain restore -i
/var/backup_directory/FIRST_INCREMENTAL
# foreman-maintain restore -i
/var/backup_directory/SECOND_INCREMENTAL
```

foreman-maintain backup コマンドを使用してバックアップを作成した場合は、**-i** オプションは必要ありません。

復元プロセスが完了するとすべてのプロセスがオンラインになり、すべてのデータベースおよびシステム設定がバックアップ時の状態に戻ります。

トラブルシューティングを行うには、**/var/log/foreman/production.log** および **/var/log/messages** にあるファイルを参照してください。

8.1. 仮想マシンのスナップショットを使用した CAPSULE SERVER のバックアップと復元

Capsule Server が仮想マシンである場合、スナップショットから復元することができます。復元元となるスナップショットは、毎週作成することが推奨されます。失敗した場合は、新規 Capsule Server をインストールまたは設定し、Satellite Server からデータベースコンテンツを同期します。

必要な場合は、新規 Capsule Server をデプロイします。ホスト名が以前のものと同じであることを確認してください。その後に Capsule 証明書をインストールします。これは Satellite Server にもある場合があり、パッケージ名が `-certs.tar` で終わるものです。もしくは、新規に作成します。CAPSULE SERVER のインストール にある手順に従い、web UI で Capsule Server が Satellite Server に接続されたことを確認します。この後に、以下の手順で Satellite Server から同期します。

外部 Capsule からの同期

1. 外部 Capsule から同期 するには、web UI で関連する組織とロケーションを選択するか、**任意の組織** と **任意のロケーション** を選択します。
2. **インフラストラクチャー** > **Capsules (スマートプロキシー)** に移動し、同期する Capsule 名をクリックします。
3. **概要** タブで **同期** を選択します。

第9章 SATELLITE SERVER および CAPSULE SERVER の名前変更

Satellite Server または Capsule Server の名前変更には、**satellite-change-hostname** スクリプトを使用します。Red Hat Satellite にはホスト名への参照が含まれており、それらの変更はこのスクリプトを使用して行います。Satellite Server の名前を変更すると、その Satellite Server 自体とすべての Capsule Server、さらに Satellite Server に登録されているすべてのホストに影響があります。Capsule Server の名前を変更すると、その Capsule Server 自体とそこに登録されている全ホストに影響があります。

警告

名前変更プロセスを実行すると、変更対象の Satellite Server 上の全サービスがシャットダウンされます。名前変更が完了すると、全サービスが再開されます。

9.1. SATELLITE SERVER の名前変更

Satellite Server のホスト名は、Satellite Server のコンポーネント、すべての Capsule Server、および Satellite Server に登録されている全ホストが通信用に使用しています。このため、Satellite Server の名前を変更すると、これらの参照を更新する必要があります。

外部認証を使用している場合は、**satellite-change-hostname** スクリプトの実行後に、外部認証向けに Satellite Server を再設定する必要があります。**satellite-change-hostname** スクリプトは、Satellite Server 用の外部認証を破棄してしまいます。外部認証の設定については、*12章 外部認証の設定* を参照してください。

前提条件

- (オプション) Satellite Server にカスタムの X.509 証明書がインストールされている場合は、ホスト名で新規証明書を取得する必要があります。全ホストを Satellite Server に再登録すると、新規証明書がインストールされます。カスタム X.509 証明書の取得については、『**オンラインネットワークからの SATELLITE SERVER のインストール**』の カスタムサーバー証明書を使用した Satellite Server の設定 を参照してください。
- Satellite Server のバックアップ。**satellite-change-hostname** スクリプトを実行すると、Satellite Server に不可逆的な変更を行います。名前変更プロセスが失敗した場合は、バックアップから復元してください。詳細は、「 Identity Management の使用」 を参照してください。

Satellite Server の名前変更

1. Satellite Server で **satellite-change-hostname** スクリプトを実行する適切なメソッドを選択して、新しいホスト名と Satellite 認証情報を提供します。
   - Satellite Server を自己署名証明書でインストールした場合は、以下を実行します。

```
# satellite-change-hostname new_satellite \
--username admin \
--password password
```

- Satellite Server を SSL 証明書でインストールした場合は、以下を実行します。

```
# satellite-change-hostname new_satellite \
--username admin \
--password password \
-c "/root/ownca/test.com/test.com.crt" \
-r "/root/ownca/test.com/test.com.crt.req" \
-k "/root/ownca/test.com/test.com.key"
```

名前変更が成功すると、******* Hostname change complete! ******* というメッセージが表示されます。

2. (オプション) Satellite Server の新しいホスト名用に新規の X.509 証明書を取得している場合は、Satellite インストールスクリプトを実行して証明書をインストールします。カスタム X.509 証明書のインストールについては、『**オンラインネットワークからの SATELLITE SERVER のインストール**』の カスタムサーバー証明書を使用した Satellite Server の設定 を参照してください。

3. 全 Capsule Server と Satellite Server に登録済みのホストで、ブートストラップ RPM を再インストールし、ホストを Satellite Server に再登録します。以下の例では、組織と環境の値をご使用の環境のものに置き換えてください。

   a.

   ```
   # yum remove -y katello-ca-consumer*
   ```

   b.

   ```
   # rpm -Uvh http://new-satellite.example.com/pub/katello-ca-
   consumer-latest.noarch.rpm
   ```

   c.

   ```
   # subscription-manager register \
   --org="Default_Organization" \
   --environment="Library" \
   --force
   ```

   このステップでは、Red Hat Satellite のリモート実行機能の使用が推奨されます。詳細は、『**ホストの管理**』の リモートジョブの設定および実行 を参照してください。

4. すべての Capsule Server、および Satellite Server に登録されている全ホストに再度サブスクリプションをアタッチして、サブスクリプションをリフレッシュします。

   a.

   ```
   # subscription-manager refresh
   ```

   b.

   ```
   # yum repolist
   ```

   このステップでは、Red Hat Satellite のリモート実行機能の使用が推奨されます。詳細は、『**ホストの管理**』の リモートジョブの設定および実行 を参照してください。

5. 全 Capsule Server で、Satellite インストールスクリプトを再実行して、新規ホスト名への参照を更新します。

```
# satellite-installer --foreman-proxy-content-parent-fqdn new-satellite.example.com \
--foreman-proxy-foreman-base-url https://new-satellite.example.com \
--foreman-proxy-trusted-hosts new-satellite.example.com
```

6. Satellite Server で、コンテンツを各 Capsule Server に同期します。

   a. すべての Capsule Server を ID 番号で一覧表示します。

```
# hammer capsule list
```

   b. 各 Capsule Server に以下のコマンドを入力します。

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

9.2. CAPSULE SERVER の名前変更

Capsule Server のホスト名は、Satellite Server のコンポーネント、すべての Capsule Server、および Capsule Server に登録されている全ホストが参照しています。このため、Capsule Server の名前を変更すると、これらの参照を更新する必要があります。

前提条件

- オプション: Capsule Server 用の新規の X.509 カスタム証明書ファイル。カスタム X.509 証明書の取得については、『**CAPSULE SERVER のインストール**』の カスタムサーバー証明書を使用した Capsule Server の設定 を参照してください。
- Capsule Server のバックアップ。**satellite-change-hostname** スクリプトを実行すると、Capsule Server に不可逆的な変更を行います。名前変更プロセスが失敗した場合は、バックアップから復元してください。
  Red Hat Satellite では、Capsule Server 用のネイティブのバックアップ方法が提供されていません。詳細は、*7章Satellite Server および Capsule Server のバックアップ*を参照してください。

Capsule Server の名前変更

1. Satellite Server で、新規証明書アーカイブファイルを作成します。デフォルトの Satellite Server 証明書を使用している場合は、以下を実行します。

```
# capsule-certs-generate --capsule-fqdn new-capsule.example.com \
--certs-tar /root/new-capsule.example.com-certs.tar
```

   .tar ファイルへの完全パスを必ず入力するようにしてください。

   a. Capsule Server でカスタムの X.509 証明書を使用している場合は、『**CAPSULE SERVER のインストール**』の Capsule サーバーの証明書アーカイブファイルの作成 を参照してください。

2. Satellite Server 上で、証明書アーカイブファイルを Capsule Server にコピーし、プロンプトが出たら、**root** ユーザーのパスワードを提供します。この例では、アーカイブファイルは **root**

ユーザーのホームディレクトリーにコピーされますが、別の場所にコピーすることもできます。

```
# scp /root/new-capsule.example.com-certs.tar
root@capsule.example.com:
```

3. Capsule Server で **satellite-change-hostname** スクリプトを実行し、新しいホスト名と Satellite 認証情報、および証明書アーカイブファイル名を提供します。

```
# satellite-change-hostname new_capsule --username admin \
--password password \
--certs-tar /root/new-capsule.example.com-certs.tar
```

.tar ファイルへの完全パスを必ず入力するようにしてください。

名前変更が成功すると、******* Hostname change complete! ******* というメッセージが表示されます。

4. (オプション) Capsule Server の新しいホスト名で新規の X.509 証明書を取得している場合は、Satellite インストールスクリプトを実行して証明書をインストールします。カスタム X.509 証明書のインストールについては、『**CAPSULE SERVER のインストール**』の Capsule Server のカスタム証明書のインストール を参照してください。

5. Capsule Server に登録済みのホストで、ブートストラップ RPM を再インストールし、ホストを Capsule Server に再登録します。以下の例では、組織と環境の値をご使用の環境のものに置き換えてください。

```
# yum remove -y katello-ca-consumer*
```

```
# rpm -Uvh http://new-capsule.example.com/pub/katello-ca-consumer-
latest.noarch.rpm
```

```
# subscription-manager register --org="Default_Organization" \
--environment="Library" \
--force
```

このステップでは、Red Hat Satellite のリモート実行機能の使用が推奨されます。詳細は、『**ホストの管理**』の ホストでのリモートジョブの実行 を参照してください。

6. Capsule Server に登録されている全ホストに再度サブスクリプションをアタッチして、サブスクリプションをリフレッシュします。

```
# subscription-manager refresh
```

```
# yum repolist
```

7. Capsule Server の名前を変更します。

   a. Satellite web UI で、**インフラストラクチャー** > **Capsules (スマートプロキシー)** に移動します。

   b. リストで Capsule Server を見つけ、その行の **編集** をクリックします。

c. **名前** と **URL** フィールドが Capsule Server の新規ホスト名に一致するように変更して、**送信** をクリックします。

8. DNS サーバーで、Capsule Server の新規ホスト名用のレコードを追加し、古いホスト名のレコードを削除します。

第10章 SATELLITE SERVER のメンテナンス

本章では、監査レコードの取り扱い、未使用タスクのクリーン方法、一杯になったディスクから Pulp を回復する方法、NongoDB からディスク領域を解放する方法、Red Hat Insights を使ってプロアクティブにシステムを診断する方法などの Red Hat Satellite Server のメンテナンス方法について説明します。

10.1. 監査レコードの削除

監査レコードは Satellite で自動作成されます。**foreman-rake audits:expire** コマンドを使うと、監査はいつでも削除できます。また、cron job を使って監査レコードの削除を希望する頻度でスケジュールすることもできます。

デフォルトでは、**foreman-rake audits:expire** コマンドを使用すると 90 日以上経過した監査レコードが削除されます。**days** オプションに日数を追加することで、監査レコードを保持する日数を指定することが可能です。

たとえば、7 日以上経過した監査レコードを削除する場合は、以下のコマンドを実行します。

```
# foreman-rake audits:expire days=7
```

10.2. 監査レコードの匿名化

foreman-rake audits:anonymize コマンドを使うと、データベースで監査レコードを保持しつつ、ユーザーアカウントや IP 情報を削除できます。また、cron job を使って監査レコードの匿名化を希望する頻度でスケジュールすることもできます。

デフォルトでは、**foreman-rake audits:anonymize** コマンドを使用すると 90 日以上経過した監査レコードが匿名化されます。**days** オプションに日数を追加することで、監査レコードを保持する日数を指定することが可能です。

たとえば、7 日以上経過した監査レコードを匿名化する場合は、以下のコマンドを実行します。

```
# foreman-rake audits:anonymize days=7
```

10.3. 未使用タスクのクリーニング

未使用タスクをクリーンアップすると、データベース内のディスクスペースを削減し、ディスク増加率を制限することができます。クリーニングを定期的に実行すると、 Satellite のバックアップがより短時間で完了し、全体的なパフォーマンスも上がります。

未使用タスクのクリーニング

インストーラーには、cron ジョブが自動で古いタスクを削除するようにする機能があります。意図しないタスクのクリーンアップを避けるために、この機能はデフォルトでは有効になっていません。

1. cron ジョブを有効にします。

   ```
   # satellite-installer --foreman-plugin-tasks-automatic-cleanup true
   ```

2. デフォルトでは、cron ジョブは毎日午後 7 時 45 分に実行するようにスケジュールされています。この時間を変更するには、**--foreman-plugin-tasks-cron-line** パラメーターの値を変更します。

```
# satellite-installer --foreman-plugin-tasks-cron-line "00 15 * * *"
```

上記のコマンドでは、cron ジョブが毎日午後 3 時に実行されるようになります。cron のフォーマットについての詳細は、**man 5 crontab** を参照してください。

全タスクが削除される頻度の変更と、cron ジョブの詳細な設定は、**/etc/foreman/plugins/foreman-tasks.yaml** ファイルのコンテンツを変更して行います。

10.4. 完全なディスクからのリカバリー

以下の手順では、Pulp データベースのある論理ボリューム (LV) に空きスペースがない場合の解決方法について説明します。

完全なディスクからのリカバリー

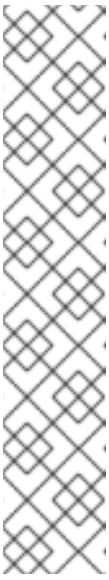
1. 実行中の Pulp タスクを完了させます。新たなタスクは開始しないでください。ディスクに空きスペースがないため、失敗することになります。
2. **/var/lib/pulp** ディレクトリーのある LV に十分な空きスペースがあることを確認します。以下のような方法があります。
   a. 孤立したコンテンツを削除します:

   ```
   # foreman-rake katello:delete_orphaned_content
   RAILS_ENV=production
   ```

   これは 1 週間ごとに実行されるので、多くのスペースが解放されるわけではありません。

   b. できるだけ多くのリポートのダウンロードポリシーを **即時** から **オンデマンド** に変更し、ダウンロード済みパッケージを削除します。手順については、カスタマーポータルの Red Hat ナレッジソリューション How to change syncing policy for Repositories on Satellite 6.2 from "Immediate" to "On-Demand" を参照してください。

   c. **/var/lib/pulp** ディレクトリーのある LV 上のファイルシステムを拡張します。詳細は、**論理ボリュームマネージャーの管理** の 論理ボリュームのファイルシステムの拡張 を参照してください。



注記

(ext3、ext4、または xfs などの) 通常外のファイルシステムを使用している場合は、そのファイルシステムをアンマウントして使用されていない状態にする必要があります。その場合、以下を実行します。

- Satellite サービスを停止します。

```
# foreman-maintain service stop
```

- LV 上のファイルシステムを拡張します。
- Satellite サービスを起動します。

```
# foreman-maintain service start
```

3. ディスクに空きスペースがないために Pulp タスクが失敗していた場合は、それらのタスクを再実行します。

10.5. MONGODB からのディスク領域の確保

MongoDB データベースは、特に負荷の高いデプロイメントにおいて、ディスク領域を大幅に使用できます。以下の手順では、このディスク領域の一部を確保する方法を説明しています。

前提条件

- MongoDB データベースのバックアップ。バックアップ作成の説明については 「Pulp コンテンツなしでのバックアップの実行」 を参照してください。
- Pulp サービスの停止。

```
# systemctl stop goferd httpd pulp_workers pulp_celerybeat \
pulp_resource_manager pulp_streamer
```

MongoDB からのディスク領域の確保

1. MongoDB シェルにアクセスします。

```
# mongo pulp_database
```

2. 修復前の MongoDB のディスク領域の使用量を確認します。

```
> db.stats()
```

3. 現在の MongoDB データベースに 2 GB を足したサイズに相当する空のディスク領域があることを確認します。MongoDB データベースを含むボリュームに十分な領域がない場合、別のボリュームをマウントし、これを修復に使用することができます。

4. 修復コマンドを入力します。

```
> db.repairDatabase()
```

データベースのサイズによっては、修復コマンドは、その他すべての操作をブロックし、完了までに時間がかかる場合があることに注意してください。

5. 修復後の MongoDB のディスク領域の使用量を確認します。

```
> db.stats()
```

6. Pulp サービスを開始します。

```
# systemctl start goferd httpd pulp_workers pulp_celerybeat \
pulp_resource_manager pulp_streamer
```

10.6. 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。

サブスクリプションマニフェストに Red Hat Insights のエンタイトルメントを追加する必要はありません。

Satellite で Red Hat Insights を使用するには、最初にホストをインストールして Red Hat Insights に登録する必要があります。

Puppet を使用して、または手動でホストをインストールおよび登録する方法については、Red Hat Insights Getting Started を参照してください。

Ansible ロールを使用した Red Hat Insights のデプロイ

RedHatInsights.insights-client Ansible ロールを使用すると、Red Hat Insights とのホストのインストールおよび登録を自動化することができます。Satellite にこのロールを追加するには、4章*Ansible ロールの管理* の手順に従ってください。

1. **RedHatInsights.insights-client** ロールをホストに追加します。新規ホストについては ホストの作成 を、希望のホストにロールを追加する方法については 既存ホストへの Ansible ロールの割り当て を参照してください。

2. **RedHatInsights.insights-client** ロールをホストで実行するには、**ホスト** > **すべてのホスト** に移動して、使用するホスト名をクリックします。

3. **Ansible ロールの実行** ボタンをクリックします。

ロール実行が完了したら、Satellite web UI の **Insights** > **概要** ページで追加したホストの表示と作業が可能になります。

追加情報

- Red Hat Insights プラグインにシステム更新を適用するには、更新後に `httpd restart` を使用します。
- Red Hat Insights およびすべてのプラグインのログを確認するには、`/var/log/foreman/production.log` に移動します。
- Red Hat Insights との接続に問題がある場合は、証明書が最新のものであることを確認してください。サブスクリプションマニフェストをリフレッシュして証明書を更新します。

第11章 問題のログとレポート

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、Satellite web UI 内でサポートケースにアクセスする方法など、Red Hat Satellite Server における問題のログおよびレポート方法について説明します。

11.1. 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11.1 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 および **/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[1] を参照してください。

11.2. デバッグロギングの有効化

本セクションでは、**デバッグロギング**を有効にして Satellite 6.4 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 6.4 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" に設定します。
   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
   ```

2. 個別ロギングタイプを選択します。
   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. Satellite サービスを再起動します。

   ```
   # foreman-maintain service restart
   ```

ロガーとそのデフォルト値の完全なリスト

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

11.3. 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11.2 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、出力される tar ファイルは、**/tmp/foreman-debug-xxx.tar.xz** に格納されます。 また、**foreman-debug** コマンドは、過去 60 日間に実行されたタスクをエクスポートします。デフォルトでは、出力される tar ファイルは、**/tmp/task-export-xxx.tar.xz** に格納されます。このファイルが見当たらない場合は、**/tmp/task-export.log** ファイルで、タスクのエクスポートが失敗した理由を確認できます。 詳細情報については、**foreman-debug --help** を実行してください。 このコマンドの実行時に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/ja/solutions/78443: **Red Hat Enterprise Linux 4.6 以降における sosreport の役割と取得方法** 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作成時に **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 では、この情報を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。

11.4. 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 サポートに送信することができます。

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既存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**

11.5. 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:** 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:** 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:** 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。

11.5.1. 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。

Red Hat Satellite Server からのソリューション検索:

1. 画面右上で、**Red Hat Access** > **検索** をクリックします。
2. 必要に応じて、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。

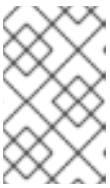
3. **Red Hat Search** フィールドに検索クエリーを入力します。検索結果が左側の **推奨項目** リストに表示されます。
4. **推奨項目** リストでソリューションをクリックします。ソリューションの記事がメインパネルに表示されます。

11.5.2. 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。

Red Hat Satellite Server からのログ診断ツールの使用:

1. 画面右上で、**Red Hat Access** > **ログ** をクリックします。
2. 必要に応じて、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 **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. **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、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すると、**Red Hat 診断** ボタンが有効になります。
6. **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. ソリューションの結果によって、以下のいずれかに従います。
   - 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、**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既存サポートケースの作成」 を参照してください。

11.5.3. 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。

Red Hat Satellite Server から既存サポートケースを表示:

1. 画面右上で、**Red Hat Access** > **サポート** > **マイケース** をクリックします。
2. 必要に応じて、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 **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。
   - **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。
   - ドロップダウンリストから、特定の **ケースグループ** を選択します。**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。
   - 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、**ケース ID** をクリックすると、サポートケースが表示されます。

11.5.4. Red Hat Access プラグインを使用した既存サポートケースの編集

Red Hat Access プラグインを使用して、Red Hat Satellite Server から既存のサポートケースを編集することができます。

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。
   - **添付ファイル:** システムからローカルファイルを添付します。分かりやすくするために、ファイル名を追加してください。

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。

   - **ケースコメント:** 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 **コメントの追加** をクリックします。

11.5.5. Red Hat Access プラグインを使用した既存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。

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

1. 画面右上で、**Red Hat Access** > **サポート** > **新規ケース** をクリックします。
2. 必要に応じて、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. **製品** および **製品バージョン** フィールドは、自動入力されます。以下のフィールドに入力します。

   - **概要** — 問題の簡単な概要を記載します。
   - **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. **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。

   - **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。
   - **ケースグループ** — 通知する必要があるメンバーに応じて、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、**ローカルファイルの添付** 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よりも大きい場合は、FTP を使用します。

7. **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、ケース番号が提供されます。

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

---

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

第12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。

警告

ユーザーおよびグループアカウントはすべて、ローカルアカウントである必要があります。これにより、Satellite Server 上のローカルアカウントと Active Directory ドメイン内のアカウントによる認証競合が避けられます。

ユーザーおよびグループアカウントが **/etc/passwd** と **/etc/group** ファイルの両方に存在すれば、この競合によってシステムが影響を受けることはありません。たとえば、**puppet**、**apache**、**foreman** および **foreman-proxy** グループのエントリーが **/etc/passwd** と **/etc/group** の両ファイルに存在することを確認するには、以下のコマンドを実行します。

```
# cat /etc/passwd | grep 'puppet\|apache\|foreman\|foreman-proxy'
# cat /etc/group | grep 'puppet\|apache\|foreman\|foreman-proxy'
```

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 の使用」 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は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、認証情報、および権限を管理します。詳細については、「 Identity Management 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。

12.1. LDAP の使用

12.1.1. TLS での セキュア LDAP (LDAPS) の設定

注記

本セクションでは直接 LDAP 統合について説明しますが、Red Hat では SSSD を使用し、IdM、AD、または LDAP サーバーに対して SSSD を設定することを推奨しています。これらの設定については、本書の他の箇所で説明しています。

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、LDAP 認証の設定: に進みます。

LDAP サーバーから証明書を取得する

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 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実行して、LDAP サーバーから取得した **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
```

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

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、Using Identity Management または Using Active Directory を参照してください。

LDAP 認証の設定:

1. allow Network Information System (NIS) サービスブール値を 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. **管理** > **LDAP 認証** に移動します。
3. **新規認証ソース** をクリックします。
4. **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 です (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. **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. **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、E 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. **ロケーション** タブで、左側の表からロケーションを選択します。選択したロケーションは、LDAP 認証ソースから作成されたユーザーに割り当てられ、初回ログイン以降、利用可能となります。
8. **組織** タブで、左側の表から組織を選択します。選択した組織は、LDAP 認証ソースから作成されたユーザーに割り当てられ、初回ログイン以降、利用可能となります。
9. **送信** をクリックします。

これで Satellite Server は LDAP サーバーを使用するように設定されました。

Satellite でアカウントを自動作成する を選択していない場合は、「ユーザーの作成」 を参照してユーザーアカウントを手動で作成してください。

こ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後に、Satellite 管理者はロールを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。

12.1.3. LDAP 設定の説明と例

以下の表は、**Account** タブの各設定の説明を示しています。

表12.1 アカウントタブの設定

設定	説明
アカウント	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。
アカウントパスワード	**アカウント** フィールドで定義されたユーザーの LDAP パスワード。**アカウント** が **$login** 変数を使用している場合は、このフィールドを空白にすることができます。
ベース DN	LDAP ディレクトリーの最上位のドメイン名。
グローバルベース 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 フィルター	LDAP クエリを制限するフィルター。例については 「LDAP フィルターの例」 を参照してください。
オンザフライ登録	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`** の警告が表示されることがあります。その場合は、ユーザーは Satellite 管理者に連絡してユーザーアカウントに適切なロールを関連付けてもらう必要があります。
Usergroup sync	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、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12.2 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
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12.3 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12.4 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
メールアドレス属性	mail

12.1.3.1. LDAP フィルターの例

管理者は LDAP フィルターを作成することで、特定のユーザーの Satellite へのアクセスを制限することができます。

表12.5 特定ユーザーのログインを許可するフィルターの例

ユーザー	フィルター
User1、User3	(memberOf=cn=Group1,cn=Users,dc=domain,dc=example)
User2、User3	(memberOf=cn=Group2,cn=Users,dc=domain,dc=example)
User1、User2、User3	(&(objectClass=user)((memberOf=cn=Group1,cn=Users,dc=domain,dc=example) (memberOf=cn=Group2,cn=Users,dc=domain,dc=example)))

LDAP ディレクトリー構造

上記の例のフィルターで使用される LDAP ディレクトリー構造

```
DC=Domain,DC=Example
   |
   |----- CN=Users
          |
          |----- CN=Group1
          |----- CN=Group2
          |----- CN=User1
          |----- CN=User2
          |----- CN=User3
```

LDAP グループメンバーシップ

上記の例のフィルターで使用されるグループメンバーシップ

グループ	メンバー
Group1	User1、User3
Group2	User2、User3

12.2. IDENTITY MANAGEMENT の使用

以下の方法のいずれかを選択します。

- 「 Identity Management の直接的な使用」
- 「LDAP 認証での Identity Management の使用」

12.2.1. Identity Management 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。

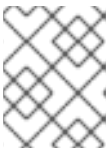
本章の例では、IdM と Satellite の設定が分かれていることを前提とします。ただし、両方のサーバーに対して管理者権限を持っている場合は、Linux ドメイン ID、認証、およびポリシーガイド[2] で説明されているように、IdM を設定できます。

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。

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、Linux ドメイン ID、認証、およびポリシーガイド[3] 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
```

ホスト設定プロパティーの詳細については、Linux ドメイン ID、認証、およびポリシーガイド[4] 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. Satellite サービスを再起動します。

```
# foreman-maintain service restart
```

この時点で、外部ユーザーは IdM 認証情報を使用して 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、Linux ドメイン ID、認証、およびポリシーガイド[5] を参照してください。

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、Red Hat カスタマーポータル上の記事 How to configure HBAC rules in IdM[6] を参照してください。

5. 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
```

12.2.2. LDAP 認証での Identity Management 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 Identity Management を使用する場合の詳細については、「LDAP の使用」 を参照してください。

12.3. ACTIVE DIRECTORY の使用

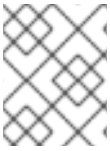
以下の方法のいずれかを選択します。

- 「Active Directory の使用」
- 「フォレスト間信頼での Active Directory の使用」
- 「LDAP 認証での Active Directory の使用」

12.3.1. Active Directory の使用

本セクションでは、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、ID が格納された AD ドメインに Satellite Server が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 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 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実行できます。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 以降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。本セクションの例では、**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 がインストールされていることを確認します。

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

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-compat krb5-workstation
```

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 に対して行ったり、Satellite のインストール中に行ったりすることができます。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。

GSS-proxy との直接 AD 統合の設定:

1. **/etc/ipa/** ディレクトリーと **default.conf** ファイルを作成します。

```
# mkdir /etc/ipa
# touch /etc/ipa/default.conf
```

2. **default.conf** ファイルに以下のコンテンツを追加します。

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

3. 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
```

4. 以下の内容で **/etc/gssproxy/00-http.conf** ファイルを作成します。

```
[service/HTTP]
mechs = krb5
cred_store = keytab:/etc/krb5.keytab
cred_store = ccache:/var/lib/gssproxy/clients/krb5cc_%U
euid = 48
```

5. 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/
```

6. keytab エントリーを作成します。

```
# KRB5_KTNAME=FILE:/etc/httpd/conf/http.keytab net ads keytab add
HTTP -U administrator -d3 -s /etc/net-keytab.conf
# chown root.apache /etc/httpd/conf/http.keytab
# chmod 640 /etc/httpd/conf/http.keytab
```

7. Satellite の IPA 認証を有効にします。

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

8. **gssproxy** サービスを起動して、有効にします。

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

9. Apache サーバーが gssproxy サービスを使用するように設定します。

   a. 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
```

   b. 変更をサービスに適用します。

```
# systemctl daemon-reload
```

10. **httpd** サービスを起動して、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。

SSO が Satellite Server で動作していることを確認するには、以下のコマンドを入力して LDAP ユーザーの Kerberos チケットを取得します。

```
# kinit ldapuser
```

Kerberos チケットを表示するには、以下のコマンドを入力します。

```
# klist
```

成功した SSO ベースの認証からの出力を表示するには、以下のコマンドを入力します。

```
# curl -k -u : --negotiate
https://satellite.example.com/users/extlogin
<html><body>You are being <a
href="https://satellite.example.com/users/4-ldapuserexample-
com/edit">redirected</a>.</body></html>
```

この時点でユーザーは Satellite UI でアクセス認証情報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、システムレベルの認証ガイド を参照してください。Internet Explorer ブラウザーを使用している場合は、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 = +foreman
```

ここでの、**foreman** は PAM サービス名です。GPO の詳細については、Windows 統合ガイド[7] を参照してください。

12.3.2. 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 との間での有効な信頼関係により、AD のユーザーは一連の認証情報を使用して 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、Windows 統合ガイド[8] を参照してください。

Satellite 側から見ると、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、「Identity Management 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
```

12.3.3. 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 の使用」 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。

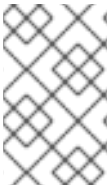
12.4. 外部ユーザーグループの設定

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。**管理** > **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 の使用」 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。

- *12章外部認証の設定* の説明のように 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
```

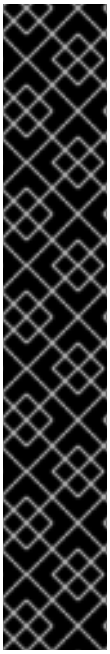
ここでの **username** は、外部グループメンバーの名前です。Satellite では、外部グループを設定する前に、少なくとも 1 人の外部ユーザーが初めて認証する必要があります。また、外部認証ソースには少なくとも 1 人のユーザーが存在する必要があります。

外部ユーザーグループの設定:

1. **管理** > **ユーザーグループ** に移動して、**新規ユーザーグループ** をクリックします。
2. **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. **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、**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. **外部グループ** タブで、**外部ユーザーグループの追加** をクリックして、**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。
   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 LDAP ソースがユーザーグループメンバーシップを同期するように設定することができます。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。

12.5. 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。

12.5.1. 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 に登録されている。
- 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る。

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、以下の出力が表示されます。

```
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動し、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。

- 外部の 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 \
--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
```

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** > **Capsules (スマートプロキシー)** に移動します。

   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、**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** に移動し、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. 以下のサブタブのフィールドに値を入力します。

      - **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。
      - **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。
      - **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。

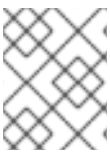
   c. **送信** をクリックします。

これで 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。次のセクションでは、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説明します。

12.5.2. 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。

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、

- **hostgroup_name** はホストグループの名前です。
- **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、

- **automember-add** は automember グループとしてグループにフラグを立てます。
- **--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。
- **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、

- **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。
- **--key=userclass** はキー属性を userclass に指定します。
- **--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。
- **--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。

- **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。

---

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

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

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

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

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

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

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

第13章 SATELLITE SERVER 機能の拡張

Red Hat Satellite Server は、プラグインをインストールし、オーケストレーションと Rails イベントにフックを使用することで、機能拡張が可能です。プラグインは、RPM パッケージとして Red Hat リポジトリーと Foreman リポジトリーから入手できます。

13.1. SATELLITE プラグイン

Satellite プラグインは以下から入手できます。

- Red Hat リポジトリー
- Foreman リポジトリー

Satellite 用のプラグインには通常、RPM パッケージ名に **`foreman`** という語が含まれており、Capsule 用のプラグインには、名前に **`smart_proxy`** が含まれています。

Red Hat が提供するプラグインは、Satellite **`CLI`** から **`yum`** コマンドを使用して検索とインストールができます。

アップストリーム の Satellite プラグインは、Foreman リポジトリーで入手できます。Foreman の各リリースには、該当リリース用のプラグインを格納している個別のリポジトリーがあります。

アップストリーム プラグインをインストールするには、Foreman リポジトリーを Satellite で設定する必要があります。設定が完了したら、**`yum`** コマンドを使用して Satellite CLI から検索とインストールができます。

Foreman リポジトリーは、http://yum.theforeman.org/plugins から入手できます。

注記

お使いのシステムにある Foreman のバージョンと互換性のあるプラグインをインストールするように注意してください。

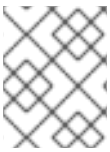
`yum info` または **`rpm -qi`** を使用すると、RPM パッケージの説明を表示してプラグインを確認することができます。

重要

Red Hat では、Foreman API はサポートしていますが、Foreman リポジトリーからインストールしたプラグインはサポートしていません。

13.1.1. プラグインの検索

Satellite **`CLI`** を使って利用可能なプラグインを検索します。



注記

アップストリーム プラグインも検索するには、Foreman リポジトリーを 「Foreman リポジトリーの設定」 の説明に従って設定します。

手順

- root ユーザーとして **yum search** を使ってパッケージ名に "-foreman" がつくパッケージを検索します。
  例 - Satellite 用 rubygem プラグインの検索

```
# 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
```

13.1.2. プラグインのインストール

Satellite CLI を使用してプラグインをインストールします。

注記

アップストリーム プラグインをインストールするには、Foreman リポジトリーを「Foreman リポジトリーの設定」 の説明に従って設定します。

手順

1. **yum install** を使用して必要なプラグインをインストールします。
   例: **tfm-rubygem-foreman_templates** プラグインのインストール:

```
# yum install tfm-rubygem-foreman_templates
```

2. **foreman-maintain** サービスを再起動します。

```
# foreman-maintain service restart
```

インストールされたことを確認するには、**yum** を使ってインストールされたプラグインを一覧表示します。

- 例: rubygem-foreman プラグインのインストール確認

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

- **yum** を使って Capsule プラグインを一覧表示することもできます。

```
# yum list installed | grep proxy
```

13.1.3. Foreman リポジトリーの設定

Satellite CLI を使用して Foreman リポジトリーを設定します。

手順

1. **rpm** コマンドで Foreman のリリースを確認します。

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

2. rpm 設定ファイルを作成します。

```
touch /etc/yum.repos.d/foreman-plugins.repo
```

3. 以下の内容をファイルに追加します。

```
[foreman-plugins]
name=Foreman plugins
baseurl=http://yum.theforeman.org/plugins/1.10/el_7_/x86_64/
enabled=1
gpgcheck=0
```

URL 内のバージョン番号 (上記の 1.10) を必要な Foreman リリース番号で置き換えます。

注記

これらのパッケージは現在 GPG 署名されていません。

foreman プラグインについての情報は、**Foreman** web サイトの Popular Plugins および List of Plugins セクションを参照してください。

13.2. FOREMAN フック

Foreman のホストオーケストレーションはフックで拡張することで、追加のタスクを実行できるようになります。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。

13.2.1. Foreman フックのインストール

Foreman フックは、デフォルトでインストールされる tfm-rubygem-foreman_hooks パッケージが提供します。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 **yum** を使用します。

手順

- **yum** 使用して foreman フックをインストールします。

```
# 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
```

13.2.2. Foreman フックの作成

Foreman フックは **/usr/share/foreman/config/hooks/** に格納されます。

手順

1. 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
```

2. 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、以下のコマンドでサブディレクトリーを作成します。

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

3. 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
```

Red Hat Enterprise Linux 7 での SELinux コンテキストは **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 7 の場合は、Fixing Problems[9] を参照してください。

13.2.3. 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。

手順

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__l
ogger.sh
#!/bin/bash
logger $1 $2
```

ファイル名 **_logger.sh** の前の数値の接頭辞 **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されます。必要に応じ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
/usr/share/foreman/config/hooks/host/managed/before_provision/_10__l
ogger.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
/usr/share/foreman/config/hooks/host/managed/before_provision/_10__l
ogger.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. Satellite サービスを再起動して、フックを登録します。

```
# foreman-maintain service restart
```

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/foreman/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",
output truncated
```

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) も一覧表示します。一般的に使用されるものは以下のとおりです。

- host
- report

13.2.4. 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、および破棄された際に、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

13.2.5. 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なると開始されます。
- **host/managed/before_provision** は、ホストで OS のインストールが完了すると、開始されます。

Rails イベントの完全なリストについては、Ruby on Rails ActiveRecord::Callbacks[10] ドキュメンテーションの「Constants」を参照してください。

13.2.6. 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満杯になり、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。

13.2.7. 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)。

---

[9] 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

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

第14章 リソースのモニタリング

本章では、管理システムのモニタリングとレポーティングの設定方法について説明します。これには、ホストの設定やコンテンツビュー、コンプライアンス、サブスクリプションと現在登録されているホスト、プロモーションおよび同期が含まれます。

14.1. RED HAT SATELLITE コンテンツダッシュボードの使用

Red Hat Satellite コンテンツダッシュボードには、ホストの設定の概要やコンテンツビュー、コンプライアンスレポート、サブスクリプションと現在登録されているホストの状態についての概要や、プロモーションおよび同期の概要、さらに最新の通知一覧などを提供する各種ウィジェットが含まれています。

コンテンツダッシュボードにアクセスするには、**モニター** > **ダッシュボード** に移動します。ダッシュボードは、各ウィジェットをクリックして別の位置にドラッグすることで、配置を変更することができます。以下のウィジェットが利用できます。

ホスト設定の状態

最後のレポーティング期間におけるホストの設定状態およびそれに該当するホスト数。以下の表では、各設定状態を説明しています。

表14.1 ホスト設定の状態

アイコン	状態	説明
	変更をエラーなく実行したホスト	最後のレポーティング期間に変更が正常に実行されたホスト。
	エラー状態のホスト	最後のレポーティング期間にエラーが検出されたホスト。
	直近 35 分間での良好なホストレポート	直近の 35 分間で変更を行わず、エラーがないホスト。
	保留中の変更があるホスト	いくつかのリソースが適用されているものの、Puppet が **noop** モードで実行されるように設定されたホスト。
	同期していないホスト	同期がされておらず、最後のレポーティング期間にレポートが受信されていないホスト。
	レポートのないホスト	最後のレポーティング期間にレポートが受信されていないホスト。
	警告が無効にされているホスト	監視対象外のホスト。

設定状態のいずれかをクリックすると、該当するホストが表示されます。

ホスト設定チャート

ホスト状態の割合と該当するホストのパーセンテージを示す円グラフ。

最新イベント

管理情報、製品、サブスクリプションの変更およびエラーに関するホストが生成するメッセージの一覧です。
すべてのユーザーに送信されるグローバル通知や、異常なアクティビティーまたはエラーを検出するためにこのセクションをモニターします。

実行分布 (直近 30 分)

デフォルトでは 30 分となっている直近の Puppet 間隔中の実行中 Puppet エージェントの分布状況を示すグラフです。このケースでは、各コラムで 3 分間にクライアントから受け取ったレポート数を示しています。

新規ホスト

最近作成されたホスト一覧。ホストをクリックすると、詳細が表示されます。

タスクのステータス

ステータスと結果別に分類される現在のすべてのタスクの概要です。タスク番号をクリックすると、対応するタスクの一覧が表示されます。

最新の警告/エラータスク

警告またはエラーにより停止している最新タスクの一覧です。タスクをクリックして詳細を確認してください。

検出されたホスト

検出プラグインによってプロビジョニングネットワークで検出されたベアメタルホストの一覧です。

最新のエラータ

Satellite に登録されているホストで利用できるすべてのエラータの一覧です。

コンテンツビュー

Satellite におけるすべてのコンテンツビューおよびそれらの公開状態の一覧です。

同期の概要

Satellite で有効にされているすべての製品またはリポジトリーおよびそれらの同期の状態の概要です。同期待ちになっている製品、同期されていない製品、同期が行われた製品はすべてこのセクションに一覧表示されます。

ホストサブスクリプションの状態

Satellite に登録されているホストによって現在使用されているサブスクリプションの概要です。サブスクリプションとはご購入いただいた証明書を指します。このサブスクリプションでホストのソフトウェア、アップグレード、およびセキュリティー修正などが利用できるようになります。以下の表はサブスクリプションの状態の種類を示しています。

表14.2 ホストのサブスクリプションの状態

アイコン	状態	説明
	**無効**	製品がインストールされていて、サブスクリプションが適切に使用されていないホストです。これらのホストには早急な対応が必要です。
	**部分使用**	サブスクリプションが使用されていて、有効なエンタイトルメントを持つホストですが、それらのエンタイトルメントは完全には使用されていません。これらのホストが予定通りに設定されていることを確認するために、これらのホストをモニターする必要があります。
	**有効**	有効なエンタイトルメントを有し、それらのエンタイトルメントを完全に使用しているホストです。

サブスクリプションタイプを選択し、選択したタイプのサブスクリプションに関連付けられたホストを表示します。

サブスクリプションのステータス

アクティブなサブスクリプションの数、次の 120 日で期限の切れるサブスクリプションの数、および最近期限切れになったサブスクリプションの数を表示する現在のサブスクリプション合計の概要です。

ホストコレクション

Satellite 内のすべてのホストコレクションとそれらの状態の一覧で、各ホストコレクション内のコンテンツホストの数なども含まれます。

Virt-who 設定の状態

環境内のホスト上で稼働している **`virt-who`** デーモンから受け取ったレポートの状態。以下の状態があります。

表14.3 Virt-who 設定状態

状態	説明
レポートなし	virt-who 設定デプロイメント中にエラーが発生したか、設定がデプロイされていないか、もしくは予定された期間に virt-who が Foreman に接続できないか、いずれかのためにレポートが受信されていません。
変更なし	ハイパーバイザーが仮想マシン上で変更を検出していない、または virt-who が予定された期間中にレポートのアップロードに失敗したために、レポートが受信されていません。仮想マシンを追加したものの、設定が **変更なし** 状態にある場合は、その virt-who が実行中か確認してください。
OK	予定期間中にエラーなしでレポートが受信されました。
設定合計数	virt-who 設定の合計数。

各状態の設定を表示するには、その設定状態をクリックします。

このウィジェットでは、**変更のない最新の設定** にある **変更なし** で最新の 3 つの設定も一覧表示されます。

最新のコンプライアンスレポート

最新のコンプライアンスレポート一覧。各コンプライアンスレポートでは、パス (P)、不合格 (F)、その他 (O) のルール数が表示されます。ホストをクリックすると、コンプライアンスレポートの詳細が表示されます。ポリシーをクリックすると、その詳細が表示されます。

コンプライアンスレポートの内訳

コンプライアンスレポートの状態の分布を示す円グラフ。

Red Hat Insights Actions

Red Hat Insights は Satellite に組み込まれたツールで、環境をチェックし、実行可能なアクションを提案します。アクションは、可用性、安定性、パフォーマンス、セキュリティーの 4 つに分けられます。

Red Hat Insights リスクサマリー

リスクレベルに応じたアクションの分布を示す表です。リスクレベルは、アクションの重要性と問題を発生させる可能性を示しています。リスクレベルには、低、中、高、重大があります。

注記

Satellite Web UI で表示される日付の形式を変更することはできません。

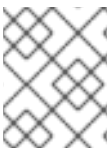
14.1.1. タスクの管理

Red Hat Satellite は、同期されたリポジトリー、適用されたエラータ、公開されたコンテンツビューなどの計画されたタスクまたは実行されたタスクのすべての詳細なログを保持します。ログを確認するには、**モニター** > **タスク** に移動します。このページから、特定のタスクを検索し、状態と詳細を確認し、(該当する場合は) エラーを出したタスクを再開できます。

タスクは Dynflow エンジンを使用して管理されます。リモートタスクには、必要に応じて調整できるタイムアウトが設定されます。

タイムアウト設定を調整するには、以下を実行します。

1. **管理** > **設定** に移動します。
2. 検索ボックスに **%_timeout** を入力し、**検索** をクリックします。検索では、説明を含む 4 つの設定が返されます。
3. **値** のコラムで、数字の横にあるアイコンをクリックして編集します。
4. 希望する秒数を入力したら、**保存** をクリックします。



注記

低帯域幅の場合は **%_finish_timeout** 値の編集が役に立つ場合があります。待ち時間が長い場合は **%_accept_timeout** 値の編集が役立つことがあります。

タスクが初期化されると、Candlepin または Pulp などのタスクで使用されるすべてのバックエンドサービスについて正常に機能するかどうかがチェックされます。チェックにパスしない場合は、次のようなエラーを受信します。

```
There was an issue with the backend service candlepin: Connection refused
- connect(2).
```

バックエンドサービスチェック機能で問題が発生する場合は、以下の方法で無効にできます。

サービスのチェックを無効にするには、以下を実行します。

1. **管理** > **設定** に移動します。
2. 検索ボックスに **check_services_before_actions** を入力し、**検索** をクリックします。
3. **値** コラムでアイコンをクリックして値を編集します。
4. ドロップダウンメニューから **false** を選択します。
5. **保存** をクリックします。

14.2. RSS 通知の設定

Satellite のイベント通知アラートを表示するには、画面右上の **通知** アイコンをクリックします。

デフォルトでは、通知エリアには Red Hat Satellite Blog で発行された RSS フィードイベントが表示されます。このフィードは 12 時間ごとに更新され、新規イベントが利用可能となると通知エリアが更新されます。

URL フィードを変更することで RSS フィード通知は設定できます。サポートされるフィード形式は、RSS 2.0 と Atom です。RSS 2.0 フィード構成の例については、Red Hat Satellite Blog feed を参照してください。Atom フィード構成の例については、Foreman blog feed を参照してください。

RSS フィード通知の設定方法

1. **管理** > **設定** に移動して、**通知** タブを選択します。
2. RSS URL の行で、**値** コラムの編集アイコンをクリックし、必要な URL を入力します。
3. RSS 有効化の行で、**値** コラムの編集アイコンをクリックし、この機能を有効または無効にします。

14.3. SATELLITE SERVER のモニタリング

Satellite Server Web UI の **概要** ページで、以下の概要情報が確認できます。

- 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

概要 ページに移動するには:

- Satellite Server web UI の右上で **管理** > **概要** をクリックします。

注記

Pulp の失敗後は、同期の遅延のため、最大 10 分間 Pulp のステータスが **エラー** ではなく、**OK** と表示される場合があります。

14.4. CAPSULE SERVER のモニタリング

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。

14.4.1. 一般的な Capsule 情報の表示

インフラストラクチャー > **Capsules (スマートプロキシー)** 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 は稼働していますか?

これは、**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?

機能 コラムで、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、『CAPSULE SERVER のインストール』 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ているか?

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 **任意の組織** を選択します。
Capsule 設定の変更後に、**アクション** コラムのドロップダウンメニューから **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。**概要** タブでは、Capsule の表にある情報と同じもの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 **管理対象ホスト** 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 コンテンツが使用している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。

14.4.2. サービスのモニタリング

インフラストラクチャー > **Capsules (スマートプロキシー)** に移動して、選択された Capsule の名前をクリックします。**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)。

14.4.3. Puppet の監視

インフラストラクチャー > **Capsules (スマートプロキシー)** に移動し、選択した Capsule 名をクリックします。 **Puppet** タブでは、以下を確認できます。

- **全般** サブタブで、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 。
- **環境** サブタブで、Puppet 環境のリスト。

Puppet CA タブでは、以下の情報を確認できます。

- **全般** サブタブで、証明書ステータスの概要と自動署名エントリーの数。
- **証明書** サブタブで、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、**取り消し** をクリックして証明書をキャンセルしたりすることができます。
- **エントリーの自動署名** サブタブで、自動署名エントリーのリスト。ここでは、**新規** をクリックしてエントリーを作成したり、**削除** をクリックしてエントリーを削除したりできます。

14.5. トレンドのモニタリング

トレンドを活用すると、Puppet レポートやファクトなど、長期にわたるインフラストラクチャーでの変更を追跡し、それらに応じたプラニングが可能になります。

トレンドを表示するには、以下の手順に従います。

1. **モニター** > **トレンド** に移動します。
2. トレンドページで、**トレンド** 一覧から選択します。

トレンドを作成するには、以下の手順に従います。

1. **モニター** > **トレンド** に移動します。
2. トレンドページで **トレンドカウンターの追加** をクリックします。
3. **トレンドタイプ** 一覧から新規トレンドのカテゴリーを選択します。
4. 該当する場合は、**Trendable** 一覧から新規トレンドの subject を選択します。
5. **名前** フィールドに 新規トレンドの名前を入力します。
6. **送信** をクリックします。

注記

これが最初のトレンドの場合は、**cron** ジョブを作成してトレンドデータを収集します。

```
# foreman-rake trends:counter
```

トレンドデータの収集頻度は、設定可能となっています。毎時 0 分に 1 時間ごとにデータを収集する場合は、以下のようにします。

```
0 * * * * /usr/sbin/foreman-rake trends:counter
```

第15章 検索およびブックマーク機能

Satellite Web UI は Web UI の大半のページで利用できる強力な検索機能を特長としています。この機能によって Satellite Server が管理するあらゆる種類のリソースを検索できます。検索では、フリーテキストと構文ベースのクエリーの両方を使用でき、クエリーは詳細な予測入力を使用して実行されます。検索クエリーは今後の再利用に備えてブックマークとして保存することができます。

15.1. 検索クエリーの構築

検索クエリーの入力を開始すると、現在のクエリーを補完する有効なオプションの一覧が表示されます。一覧からオプションを選択するか、補完機能を使用してクエリーを構築するか、または入力を継続するかのいずれかのオプションを選択できます。検索エンジンがフリーテキストを解釈する方法については、「フリーテキスト検索の使用」 を参照してください。

15.1.1. クエリーの構文

パラメーター、演算子、値

検索に利用できるフィールド、リソースおよびクエリーが解釈される方法はコンテキスト、つまり検索を実行するページによって異なります。たとえば、「ホスト」ページの「ホストグループ」フィールドは「ホストグループ」ページの「名前」フィールドに相当します。またフィールドのタイプにより、利用可能な演算子および許可される値が決まります。すべての演算子の一覧については、演算子 を参照してください。値の形式についての説明は、値 を参照してください。

15.1.2. 演算子

パラメーター と **値** の間で使用できるすべての演算子は以下の表に一覧表示されています。予測に基づいて構築されるクエリーで表示される可能性のある他の記号および特殊文字 (コロンなど) には特別な意味がなく、フリーテキストとして処理されます。

表15.1 検索で使用できる比較演算子

演算子	ショートネーム	説明	例
=	EQUALS	数値、時間的な値 (temporal value) またはテキストの値を受け入れます。テキストの場合、大文字と小文字が区別された完全一致が返されます。	`hostgroup = RHEL7`
!=	NOT EQUALS		
~	LIKE	テキストまたは時間的な値 (temporal value) を受け入れます。大文字と小文字を区別しない一致を返します。1 文字の場合の _、ゼロを含む任意の数の文字の場合の % または たは * などのワイルドカードを受け入れます。ワイルドカードが指定されない場合、文字列はワイルドカードで囲まれている場合の様に処理されます (例: %rhel7%)。	`hostgroup ~ rhel%`
!~	NOT LIKE		

演算子	ショートネーム	説明	例
>	GREATER THAN	数値、または時間的な値 (temporal value) を受け入れます。時間的な値の場合、演算子 > is は「later than (次の日付より後)」として、< は「earlier than (次の日付より前)」として解釈されます。どちらの演算子も EQUALS: >= <= と組み合わせることができます。	**registered_at > 10-January-2017** 検索結果では、指定された日付の後、つまり 2017 年 1 月 10 日から現在までの間に登録されたホストが返されます。 **registered_at <= Yesterday** 検索結果では、昨日または昨日よりも前に登録されたホストが返されます。
<	LESS THAN		
^	IN	SQL の場合と同様に、値の一覧に対して式を比較します。値が含まれる一致または値の含まれない一致をそれぞれ返します。	**release_version !^ 7**
!^	NOT IN		
HAS or set?		存在する値、または存在しない値をそれぞれ返します。	**has hostgroup** または **set? hostgroup** 「Puppet クラス」ページでは、検索は 1 つ以上のホストグループに割り当てられるクラスを返します。 **not has hostgroup** または **null? hostgroup** ホストの概要が示される「ダッシュボード」では、検索はホストグループが割り当てられていないすべてのホストを返します。
NOT HAS or null?			

記述された構文に従う単純なクエリーを組み合わせて、論理演算子の AND、OR および NOT を使用してより複雑なクエリーにすることができます。演算子の代替表記も使用できます。

表15.2 検索で使用できる論理演算子

演算子	代替表記			例
and	&	&&	<空白文字>	**class = motd AND environment ~ production**
or	|	||		**errata_status = errata_needed || errata_status = security_needed**
not	–	!		**hostgroup ~ rhel7 not status.failed**

15.1.3. 値

テキストの値

空白文字を含むテキストは引用符で囲む必要があります。囲まないと、空白は AND 演算子として解釈されます。
例:

```
hostgroup = "Web servers"
```

検索は、「Web Servers」という名前の割り当て済みのホストグループと共にホストを返します。

```
hostgroup = Web servers
```

検索は、 %servers% に一致するフィールドを持つホストグループ Web のホストを返します。

時間の値

以下を含め、数多くの日付/時刻形式を使用できます。

- "10 January 2017"
- "10 Jan 2017"
- 10-January-2017
- 10/January/2017
- "January 10, 2017"
- 「Today」、「Yesterday」など。

警告

02/10/2017 または 10-02-2017 などのあいまいな日付形式を使用しないようにしてください。

15.2. フリーテキスト検索の使用

フリーテキストを入力する際、複数のフィールドにまたがって検索が実行されます。たとえば、「64」と入力する場合、検索は名前、IP アドレス、MAC アドレスおよびアーキテクチャーにこの数字が含まれるすべてのホストを返します。

注記

複数の語句からなるクエリーは引用符で囲む必要があります。囲まないと、空白文字は AND 演算子として解釈されます。

検索はすべてのフィールドで実行されるため、フリーテキストの検索結果は非常に正確になりますが、多数のホストで実行する場合などには検索スピードが遅くなる可能性があります。このため、可能な限りフリーテキストを使用せず、より具体的で、構文ベースのクエリーを使用することが推奨されます。

15.3. ブックマークの管理

検索クエリーをブックマークとして保存し、再利用することもできます。ブックマークは削除したり、変更したりすることもできます。

ブックマークは、作成されたページでのみ表示されます。一部のページには、すべての **アクティブ** または **無効な**ホストなど、一般的な検索で使用可能なデフォルトのブックマークがあります。

15.3.1. ブックマークの作成

本セクションでは、検索クエリーをブックマークとして保存する方法について説明します。関連ページ用の検索クエリーのブックマークは、作成したそのページで保存する必要があります。たとえば、ホスト関連の検索クエリーは、ホストページで保存します。

ブックマークを作成するには、以下の手順に従います。

1. ブックマークを作成するページに移動します。
2. **検索** フィールドに保存する検索クエリーを入力します。
3. **検索** ボタンの右側にある矢印を選択し、**この検索をブックマーク** を選択します。
4. **名前** フィールドに 新規ブックマークの名前を入力します。
5. **検索クエリー** フィールドに正しい検索クエリーがあることを確認します。
6. **公開** チェックボックスの設定を確認します。
   - **公開** にチェックを入れると、ブックマークが公開されて全ユーザーに見えるようになります。
   - **公開** のチェックを外すと、ブックマークが非公開となり、作成したユーザーのみに見えるようになります。
7. **送信** をクリックします。

作成されたことを確認するには、**検索** ボタンの右側にある矢印を選択してブックマーク一覧を表示するか、**管理** > **ブックマーク** に移動してから、ブックマークの名前を **ブックマーク** 一覧で確認します。

15.3.2. ブックマークの削除

ブックマークは、ブックマークページで削除できます。

ブックマークの削除手順

1. **管理** > **ブックマーク** に移動します。
2. ブックマークページで、削除するブックマークの **削除** をクリックします。
3. 確認ウィンドウが表示されたら、**OK** をクリックして削除を確認します。

削除されたことを確認するには、ブックマークの名前がないことを **ブックマーク** 一覧で確認します。

付録A SATELLITE の設定

Red Hat Satellite Server の設定は、**管理** > **設定** ページで確認できます。

表A.1 Satellite の設定

タブ	設定	デフォルト値	説明
プロビジョニング	**名前ジェネレーターのタイプ**	**Random-based**	新規ホスト作成時のホスト名の生成方法を指定します。 デフォルトの **Random-based** オプションでは、使用可能ではあるものの必須ではない、一意のランダムなホスト名を生成します。多くのホストを作成し、命名方法が分からないユーザーには便利です。 **MAC-based** オプションは、ベアメタルのホストのみになります。ホストを削除してから、後で作成すると、MAC アドレスをベースにした同じホスト名が付けられます。サーバーを再利用し、常に同じホスト名にしたい場合に便利です。 **Off** オプションでは、名前生成関数が無効になり、ホスト名フィールドは空白になります。
	Safemode レンダリング	**Yes**	プロビジョニングテンプレートのセーフモードでのレンダリングを有効にします。 デフォルトのオプションは **Yes** で、こちらが推奨されます。変数と Satellite 内でホワイトリスト化されていないオブジェクトへのアクセスを拒否します。 **No** に設定すると、テンプレート機能を使用するパーミッションがあるユーザーは、テンプレートやパラメーター、スマート変数を編集することで、いかなるオブジェクトにもアクセスすることが可能になります。こうなると、ユーザーは Satellite Server で完全なリモートコード実行が可能になり、すべての認証が無効になることになります。特に大企業では、このオプションは安全ではありません。
全般	**DB キャッシュの修正**	**No**	Satellite は、パーミッションとロールのキャッシュを保持します。これを**Yes** に設定すると、Satellite は、次回再起動時にこのキャッシュを再作成します。