



Red Hat Satellite 6.6

Red Hat Satellite の管理

Red Hat Satellite の管理ガイド

Red Hat Satellite 6.6 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

Copyright © 2020 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

概要

本ガイドでは、Red Hat 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. KATELLO ルート CA 証明書のインストール	6
1.2. SATELLITE へのログイン	6
1.3. SATELLITE WEB UI のナビゲーションタブ	7
1.4. パスワードの変更	8
1.5. 管理ユーザーパスワードのリセット	8
1.6. 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. ANSIBLE 変数のインポート	17
4.3. ANSIBLE 変数の作成	17
4.4. SATELLITE での ANSIBLE 変数のオーバーライド	18
4.5. RED HAT ENTERPRISE LINUX システムロールの追加	19
第5章 ユーザーとロールの管理	21
5.1. ユーザー管理	21
5.1.1. ユーザーの作成	21
5.1.2. ユーザーへのロールの割り当て	22
5.1.3. SSH キー	23
5.1.4. ユーザーの SSH キー管理	23
5.1.5. 電子メール通知	24
5.1.6. E メール通知の設定	25
5.1.7. 電子メールの配信テスト	25
5.1.8. 電子メール通知のテスト	26
5.1.9. 通知タイプ	26
5.2. ユーザーグループの作成と管理	26
5.2.1. ユーザーグループ	27
5.2.2. ユーザーグループの作成	27
5.2.3. ユーザーグループの削除	27
5.3. ロールの作成および管理	27
5.3.1. ロールの作成	28
5.3.2. ロールのクローン作成	28
5.3.3. ロールへのパーミッションの追加	28
5.3.4. ロールのパーミッションの表示	29
5.3.5. パーミッションの完全テーブルの作成	29
5.3.6. ロールの削除	30
5.3.7. Satellite で利用可能な事前定義済みロール	30
5.4. 詳細なパーミッションフィルタリング	32
5.4.1. 詳細なパーミッションフィルター	32
5.4.2. 詳細なパーミッションフィルターの作成	33
5.4.3. 詳細なパーミッションフィルターの使用例	33
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	33

5.4.3.2. 組織固有のマネージャーロールの作成	34
5.4.4. 詳細な検索に対してサポートされる演算子	34
第6章 セキュリティーコンプライアンスの管理	36
6.1. セキュリティーコンテンツの自動化プロトコル	36
6.1.1. SCAP コンテンツ	36
6.1.2. XCCDF プロファイル	36
6.1.2.1. 利用可能な XCCDF プロファイルの一覧表示	36
6.2. SCAP コンテンツの設定	37
6.2.1. OpenSCAP Puppet モジュールのインポート	37
6.2.2. デフォルト OpenSCAP コンテンツのロード	37
6.2.3. 追加の SCAP コンテンツ	37
6.2.3.1. 追加の SCAP コンテンツのアップロード	37
6.3. コンプライアンスポリシーの管理	38
6.3.1. コンプライアンスポリシー	38
6.3.2. コンプライアンスポリシーの作成	38
6.3.3. コンプライアンスポリシーの表示	39
6.3.4. コンプライアンスポリシーの編集	39
6.3.5. コンプライアンスポリシーの削除	40
6.4. テーラリングファイル	40
6.4.1. テーラリングファイルのアップロード	40
6.4.2. テーラリングファイルのポリシーへの割り当て	40
6.5. OPENSAP 用のホストグループの設定	41
6.6. OPENSAP のホスト設定	42
6.7. コンプライアンスの監視	43
6.7.1. コンプライアンスポリシーダッシュボード	43
6.7.2. コンプライアンスポリシーダッシュボードの表示	43
6.7.3. コンプライアンスのメール通知	44
6.7.4. コンプライアンスレポート	44
6.7.5. ホストのコンプライアンス違反の調査	45
6.7.6. コンプライアンスレポートの検索	46
6.7.7. コンプライアンスレポートの削除	47
6.7.8. 複数のコンプライアンスレポートの削除	47
6.8. OPENSAP でサポートされる仕様	47
第7章 強度の低い暗号化の無効化	49
7.1. 強度の低い SSL 2.0 および SSL 3.0 暗号化の無効化	49
7.2. 64 ビットブロックサイズ暗号スイート (SWEET32) の無効化	50
第8章 SATELLITE SERVER および CAPSULE SERVER のバックアップ	52
8.1. SATELLITE のバックアップ	52
8.2. 完全バックアップ	53
8.2.1. 完全バックアップサイズの見積もり	53
8.2.2. 完全バックアップのオフライン実行	54
8.2.3. 完全バックアップのオンライン実行	55
8.3. 増分バックアップ	56
8.3.1. 増分バックアップのオフライン実行	56
8.3.2. 増分バックアップのオンライン実行	56
8.4. PULP コンテンツを含まないバックアップ	57
8.4.1. Pulp コンテンツを含まないバックアップのオフライン実行	57
8.4.2. Pulp コンテンツを含まないバックアップのオンライン実行	58
8.5. スナップショットのバックアップ	58
8.5.1. スナップショットバックアップの実行	58
8.6. 従来のバックアップ	59

8.7. バックアップデータ圧縮率	59
8.8. バックアップユーティリティの追加オプション	60
8.9. オフラインバックアップのスケジュール設定のスク립ト例	60
8.10. バックアップの方法と種類	61
第9章 バックアップからの SATELLITE SERVER または CAPSULE SERVER の復元	62
9.1. 完全バックアップからの復元	62
9.2. 増分バックアップからの復元	63
9.3. 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	63
9.3.1. 外部 Capsule からの同期	64
第10章 SATELLITE SERVER または CAPSULE SERVER の名前の変更	65
10.1. SATELLITE SERVER の名前の変更	65
10.2. CAPSULE SERVER の名前の変更	66
第11章 SATELLITE SERVER のメンテナンス	69
11.1. 監査レコードの削除	69
11.2. 監査レコードの匿名化	69
11.3. 未使用タスクのクリーニング機能の設定	69
11.4. 完全なディスクからのリカバリー	70
11.5. MONGODB からのディスク領域の確保	71
11.6. SATELLITE SERVER のベースオペレーティングシステムでのパッケージの管理	72
第12章 問題のログとレポート	74
12.1. デバッグロギングの有効化	74
12.2. 個別のロガーの有効化	74
12.3. ジャーナルへのロギングの設定	75
12.4. SATELLITE が提供するログファイルディレクトリー	75
12.5. ログ情報の収集ユーティリティ	76
第13章 外部認証の設定	78
13.1. LDAP の使用	79
13.1.1. セキュア LDAP 向けの TLS の設定	79
13.1.2. Red Hat Satellite で LDAP を使用するように設定する手順	80
13.1.3. LDAP 設定の説明	81
13.1.4. LDAP 接続の設定例	81
13.1.5. LDAP フィルターの例	82
13.2. IDENTITY MANAGEMENT の使用	83
13.2.1. Satellite Server での IdM 認証の設定	84
13.2.2. ホストベースの認証制御の設定	85
13.3. ACTIVE DIRECTORY の使用	86
13.3.1. GSS-Proxy	86
13.3.2. Satellite Server の AD サーバーへの登録	87
13.3.3. GSS-proxy を使用した直接 AD 統合の設定	87
13.3.4. Web ブラウザーでの Kerberos の設定	89
13.3.5. フォレスト間の信頼関係のある Active Directory	90
13.3.6. フォレスト間信頼を使用する IdM サーバーの設定	90
13.4. 外部ユーザーグループの設定	91
13.5. LDAP の外部ユーザーグループのリフレッシュ	91
13.6. IDM または AD の外部ユーザーグループのリフレッシュ	92
13.7. プロビジョンされたホストの外部認証	92
第14章 リソースの監視	96
14.1. RED HAT SATELLITE コンテンツダッシュボードの使用	96
14.1.1. タスクの管理	99

14.2. RSS 通知の設定	100
14.3. SATELLITE SERVER の監視	100
14.4. CAPSULE SERVER の監視	101
14.4.1. 一般的な Capsule 情報の表示	101
14.4.2. サービスの監視	101
14.4.3. Puppet の監視	102
14.5. トレンドの監視	102
第15章 検索およびブックマーク機能	104
15.1. 検索クエリーの構築	104
15.1.1. クエリーの構文	104
15.1.2. 演算子	104
15.1.3. 値	105
15.2. フリーテキスト検索の使用	106
15.3. ブックマークの管理	107
15.3.1. ブックマークの作成	107
15.3.2. ブックマークの削除	107
付録A SATELLITE の設定	108

第1章 RED HAT SATELLITE へのアクセス

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。

1.1. KATELLO ルート CA 証明書のインストール

Satellite に初めてログインする場合は、デフォルトの自己署名証明書を使用していることを通知する警告が表示され、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 に接続できない可能性があります。以下の手順を実行して、Satellite 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。

前提条件

Red Hat Satellite がインストールされ、設定されていること。

手順

1. Satellite Server の完全修飾ドメイン名を特定します。

```
# hostname -f
```

2. Web ブラウザーで以下の完全修飾ドメイン名を指定して Satellite Server の **pub** ディレクトリーにアクセスします。

```
https://satellite.example.com/pub
```

3. Satellite に初めてアクセスする場合は、信頼できない接続を警告するメッセージが Web ブラウザーに表示されます。自己署名証明書を承認し、Satellite の URL をセキュリティー例外として追加し、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。セキュリティー例外を承認する前に Satellite の URL が有効であることを確認します。
4. **katello-server-ca.crt** を選択します。
5. 証明書を認証局としてブラウザーにインポートして信頼し、Web サイトを特定します。

Katello ルート CA 証明書の手動インポート

ブラウザーでセキュリティー例外を追加できない場合は、Katello ルート CA 証明書を手動でインポートします。

1. Satellite CLI から、Web UI へのアクセスに使用するマシンに、**katello-server-ca.crt** ファイルをコピーします。

```
# scp /var/www/html/pub/katello-server-ca.crt \  
username@hostname:remotefile
```

2. ブラウザーで、**katello-server-ca.crt** 証明書を認証局としてインポートして信頼し、Web サイトを識別します。

1.2. SATELLITE へのログイン

さらに設定するには、Web ユーザーインターフェースを使用して Satellite にログインします。

前提条件

ブラウザーに Katello ルート CA 証明書がインストールされていること。詳細は、「[Katello ルート CA 証明書のインストール](#)」を参照してください。

手順

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/`

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。設定プロセス時にユーザーを作成されなかった場合には、デフォルトのユーザー名 **admin** が使用されます。ログインに問題がある場合は、パスワードをリセットできます。詳細は、「[管理ユーザーパスワードのリセット](#)」を参照してください。

1.3. SATELLITE WEB UI のナビゲーションタブ

ナビゲーションタブを使用して、Satellite Web UI を参照します。

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。
監視	サマリーダッシュボードおよびレポートを表示します。
Content (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。
ホスト	ホストインベントリ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。
Insights	Red Hat Insights 管理ツールを提供します。
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せん。
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。

1.4. 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。

1.5. 管理ユーザーパスワードのリセット

以下の手順を使用して、管理者パスワードを無作為に生成された文字にリセットするか、新しい管理者パスワードを設定します。

管理ユーザーパスワードのリセット:

パスワードを無作為に生成された文字にリセットするには、次の手順を実行します。

1. Satellite Server がインストールされているベースのオペレーティングシステムにログインします。
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. このパスワードを使用して、Satellite Web UI でパスワードをリセットします。
4. Satellite Server の `~/.hammer/cli.modules.d/foreman.yml` ファイルに、新規パスワードを追加します。

```
# vi ~/.hammer/cli.modules.d/foreman.yml
```

`~/.hammer/cli.modules.d/foreman.yml` ファイルを更新しない限り、Hammer CLI では新規パスワードを使用できません。

新規の管理ユーザーパスワードの設定:

管理ユーザーのパスワードを新しいパスワードに変更するには、次の手順を実行します。

1. Satellite Server がインストールされているベースのオペレーティングシステムにログインします。
2. パスワードをリセットするには、以下のコマンドを入力します。

```
# foreman-rake permissions:reset password=new_password
```

3. Satellite Server の `~/.hammer/cli.modules.d/foreman.yml` ファイルに、新規パスワードを追加します。

```
# vi ~/.hammer/cli.modules.d/foreman.yml
```

`~/.hammer/cli.modules.d/foreman.yml` ファイルを更新しない限り、Hammer CLI では新規パスワードを使用できません。

1.6. ログインページでのカスタムメッセージの設定

ログインページへのカスタムメッセージの設定

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行うことができます。
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 には、コマンドラインから Satellite サービスを管理するために **satellite-maintain service** コマンドが含まれています。このコマンドは Satellite のバックアップの作成時に役に立ちます。バックアップ作成に関する詳細は、「[Satellite 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て有効になります。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。

```
# satellite-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。

```
# satellite-maintain service status
```

satellite-maintain サービスを停止するには、以下のコマンドを実行します。

```
# satellite-maintain service stop
```

satellite-maintain サービスを起動するには、以下のコマンドを実行します。

```
# satellite-maintain service start
```

satellite-maintain 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。

```
# satellite-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があります。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ーします。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。

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

MongoDB の場合は、以下のコマンドを実行します。

```
# satellite-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参照するように設定します。

FIPS 関連の制限

[BZ#1743706](#) が解決されるまで、FIPS モードの Satellite で外部の MongoDB は使用できません。

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 サーバーの場合は、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 サーバーの場合は、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 Server と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 データベースが原因でパフォーマンスの低下が生じている可能性がある場合は、「[Satellite 6: How to enable postgres query logging to detect slow running queries](#)」を参照して時間のかかっているクエリーがあるかどうか判定します。1秒以上かかるクエリーがある場合は、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。時間のかかっているクエリーがある場合は、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ンニングします。

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参照するようにし、**satellite-installer** を実行します。

データベースをインストールするための Red Hat Enterprise Linux Server 7 の準備

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。

Red Hat Software Collections および Red Hat Enterprise Linux のサブスクリプションでは、外部データベースと Satellite を併用する場合に、正しいサービスレベルアグリーメントが提供されません。外部データベースに使用するベースシステムに、Satellite サブスクリプションもアタッチする必要があります。

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 インフラストラクチャサブスクリプションのアタッチ](#)」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を無効にし、以下のリポジトリ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-rhsc7-7-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 (RHSC) リポジトリ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 rh-mongodb34-syspaths
```

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 pulp_database \
--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 からデータベースにアクセスできることをテストします。接続が成功すると、コマンドから **1** が返ります。

```
# 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 リポジトリ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 リポジトリ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
```

- 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 = '*'
```

- /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
```

- 以下の行を追加します。

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

- postgreSQL** サービスを再起動して、変更を適用します。

```
# systemctl restart postgresql
```

- 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
```

- 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;
```

- 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
```

- postgres** ユーザーをログアウトします。

```
# \q
```

- Satellite Server から、データベースにアクセスできることをテストします。接続に成功した場合には、コマンドは **1** を返します。

```
# 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方法

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。

- Satellite Server で、**satellite-maintain** サービスを停止します。

```
# satellite-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。

```
# satellite-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='Foreman_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_user --
password pulp_password /var/migration_backup/mongo_dump/pulp_database/
```

5. **satellite-installer** コマンドを使って Satellite が新規データベースを参照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 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. ANSIBLE 変数のインポート

Ansible ロールは、変数を使用して、システムの IP アドレスを特定し、別のシステムで設定値として使用する必要がある場合など、具体的な要件があるシステムの設定を微調整します。

Ansible Playbook で Ansible 変数を使用する場合は、Capsule から Ansible 変数をインポートする必要があります。

手順

Ansible ロールの変数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 > 変数** に移動します。
2. ウィンドウの右上で、インポートする Ansible 変数を含む Capsule を選択します。
3. インポートする Ansible 変数を選択して、**更新** をクリックします。

4.3. ANSIBLE 変数の作成

Ansible ロールは、変数を使用して、具体的な要件のあるシステムの設定を微調整します。

通常、使用する Ansible ロール用に Ansible 変数をインポートします。システム設定をさらに調整する必要がある場合には、Satellite で Ansible 変数を作成することも可能です。

手順

1. Satellite Web UI で、**設定 > 変数** に移動します。
2. 右上隅で **新規 Ansible 変数** をクリックします。
3. キー フィールドで、変数の名前を入力します。この名前が Ansible ロール名を参照していることを確認します。
4. **説明** フィールドには、変数の説明を入力します。
5. **Ansible ロール** リストから、Ansible ロールを選択して変数を関連付けます。
6. オプション: Satellite で Ansible 変数をオーバーライドする方法は、[「Satellite での Ansible 変数のオーバーライド」](#) を参照してください。
7. Ansible 変数を保存するには、**送信** をクリックします。

4.4. SATELLITE での ANSIBLE 変数のオーバーライド

Satellite で Ansible ロールを実行する場合には、Satellite を使用して、Ansible 変数よりも Ansible ロールを優先させます。

変数のオーバーライドの優先順位

Ansible ロールを使用して、**Effective User** 以外のユーザーとしてタスクを実行する場合、Ansible 変数をオーバーライドするための厳密な優先順位があります。オーバーライドする変数が正しい優先順位に従っていることを確認するには、『[Ansible User Guide](#)』の「[Variable precedence: Where should I put a variable?](#)」を参照してください。

前提条件

Satellite に Ansible 変数がある。

Ansible 変数をインポートする方法は、[「Ansible 変数のインポート」](#) を参照してください。

Ansible 変数を作成する方法は、[「Ansible 変数の作成」](#) を参照してください。

以下の手順は、ホストとホストグループに触れます。ホストとホストグループの詳細は、『[ホストの管理](#)』ガイドを参照してください。

手順

Ansible 変数をオーバーライドするには、次の手順を実行します。

1. Satellite Web UI で、**設定 > 変数** に移動します。
2. Satellite でオーバーライドし、管理する Ansible 変数を選択します。
3. **デフォルトの動作** エリアに移動して、**上書き** チェックボックスを選択します。
4. **パラメータータイプ** から、**文字列** または **ブール型** 変数など、検証する値タイプを選択します。
5. **デフォルト値** フィールドで、変数と一致するものがない場合に使用するデフォルト値を入力します。
6. オプション: Ansible 変数をプレーンテキストで表示したくない場合は、**値の非表示** のチェックボックスを選択し、Satellite Web UI で変数のコンテンツをアスタリスクとして表示します。

7. オーバーライド設定を保存するには、**送信** をクリックします。

Ansible 変数を使用するには、ホストまたはホストグループにパラメーターとして変数を追加するか、グローバルパラメーターとして変数を追加します。

ホストグループの場合:

1. Web UI で、**設定** > **ホストグループ** に移動し、使用するホストグループ名を選択します。
2. **パラメーター** タブをクリックして、**ホストのグループパラメーター** のエリアで、**パラメーターの追加** をクリックします。
3. **名前** フィールドに、Ansible 変数名を追加します。
4. **タイプ** リストから、検証する変数タイプを選択します。
5. **値** フィールドで、変数の値を入力します。

ホストの場合:

1. Satellite Web UI で **ホスト** > **すべてのホスト** に移動して、使用するホストで、**編集** ボタンをクリックします。
2. **パラメーター** タブをクリックして、**ホストのパラメーター** のエリアで、**パラメーターの追加** をクリックします。
3. **名前** フィールドに、Ansible 変数名を追加します。
4. **タイプ** リストから、検証する変数タイプを選択します。
5. **値** フィールドで、変数の値を入力します。

グローバルパラメータとして追加する手順:

1. Satellite Web UI で **設定** > **グローバルパラメーター** に移動して、**パラメーターの作成** をクリックします。
2. **名前** フィールドに、Ansible 変数名を追加します。
3. **タイプ** リストから、検証する変数タイプを選択します。
4. **値** フィールドで、変数の値を入力します。
5. オプション: Ansible 変数をプレーンテキストで表示したくない場合は、**値の非表示** のチェックボックスを選択し、Satellite Web UI で変数のコンテンツをアスタリスクとして表示します。

4.5. 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 サブシステムの設定インターフェースで、Red Hat Enterprise Linux システムロールを利用すると Satellite に Ansible ロールを追加できます。Satellite で 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。

Extras チャンネルに登録する前に、「[Red Hat Enterprise Linux Extras の製品ライフサイクル](#)」の記事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。

```
# satellite-maintain packages 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. 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。
4. 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「[既存のホストへの 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て、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

この手順を使用してユーザーを作成します。

手順

ユーザーを作成するには、以下の手順を行います。

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、ユーザーの実名を入力します。
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: [13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。

CLI をご利用の場合

以下のコマンドを実行してユーザーを作成します。

```
# hammer user create \
--login user_name \
--password user_password \
--mail user_mail \
--auth-source-id 1 \
--organization-ids org_ID1,org_ID2...
```

--auth-source-id 1 の設定は、ユーザーは内部で認証されることを意味します。代わりに外部認証を指定することもできます。**--admin** オプションを追加して、管理者権限をユーザーに付与します。組織 ID を指定する必要はありません。**update** サブコマンドを使用してユーザーの詳細を変更できます。

ユーザー関連のサブコマンドに関する情報は、**hammer user --help** の入力してください。

5.1.2. ユーザーへのロールの割り当て

この手順を使用して、ロールをユーザーに割り当てます。

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。

CLI をご利用の場合

ユーザーにロールを割り当てるには、次のコマンドを入力します。

```
# hammer user add-role --id user_id --role role_name
```

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

この手順を使用して、ユーザーの SSH キーを追加または削除します。

前提条件

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. 確認プロンプトで **OK** をクリックします。

CLI をご利用の場合

SSH キーをユーザーに追加するには、公開 SSH キーファイルへのパスを指定するか、クリップボードにコピーする公開 SSH キーのコンテンツへのパスが必要です。

- 公開 SSH キーファイルがある場合は、次のコマンドを入力します。

```
# hammer user ssh-keys add \
--user-id user_id \
--name key_name \
--key-file ~/.ssh/id_rsa.pub
```

- SSH 公開キーのコンテンツがある場合は、次のコマンドを入力します。

```
# hammer user ssh-keys add \
--user-id user_id \
--name key_name \
--key ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNtYAAABBBHHS2KmNylYa2
7Qaa7EHp+2I99ucGStx4P77e03ZvE3yVRJEFikpoP3MJtYYfle8k
1/46MTIZo9CPTX4CYUHeN8= host@user
```

ユーザーの SSH キーを削除するには、次のコマンドを入力します。

```
# hammer user ssh-keys delete --id key_id --user-id user_id
```

ユーザーにアタッチされた SSH キーを表示するには、次のコマンドを入力します。

```
# hammer user ssh-keys info --id key_id --user-id user_id
```

ユーザーにアタッチされた SSH キーを表示するには、以下のコマンドを入力します。

```
# hammer user ssh-keys list --user-id user_id
```

5.1.5. 電子メール通知

電子メール通知は 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
- リポジトリの同期

デフォルトでは、ユーザーには電子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、デフォルトで送信メールが有効ではないため、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 で電子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。電子メール通知は、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ーを記入すると、**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. 電子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. **電子メール設定** タブで **テストメール** をクリックします。
ユーザーの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。

電子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. 電子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。
- **ホストエラーアドバイザー**: 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のサマリー。
- **OpenSCAP ポリシーサマリー**: OpenSCAP ポリシーレポートとその結果のサマリー。
- **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のサマリーが含まれます。これにより、どの更新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サマリーが含まれます。

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

以下の手順を使用し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。

CLI をご利用の場合

ユーザーグループを作成するには、次のコマンドを入力します。

```
# hammer user-group create \  
--name usergroup_name \  
--user-ids user_ID1,user_ID2... \  
--role-ids role_ID1,role_ID2...
```

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ラー式が提供されます（「[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

以下の手順を使用し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。

CLI をご利用の場合

以下のコマンドを実行してロールを作成します。

```
# hammer role create --name role_name
```

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

以下の手順を使用して、ロールにパーミッションを追加します。

手順

1. **管理** > **ロール** に移動します。

- 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。
- 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。
- 選択するパーミッションを **パーミッション** リストからクリックします。
- 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、すで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。
- 次へ** をクリックします。
- 送信** をクリックして変更を保存します。

CLI をご利用の場合

ロールにパーミッションを追加するには、以下の手順を実行します。

- 利用可能な全パーミッションを表示します。

```
# hammer filter available-permissions
```

- ロールにパーミッションを追加します。

```
# hammer filter create \
--role role_name \
--permission-ids perm_ID1,perm_ID2...
```

ロールとパーミッションパラメーターの詳細は、**hammer role --help** および **hammer filter --help** コマンドを入力します。

5.3.4. ロールのパーミッションの表示

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

- 管理** > **ロール** に移動します。
- 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。

```
# satellite-maintain packages 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 {|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. 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 のルールを追加して編集します。
Access Insights Viewer	Insight レポートを表示します。
Ansible Roles Manager	ホストおよびホストグループでのロールのプレイ。Ansible ロールの表示、破棄、インポートを行い、Ansible 変数を表示、編集、作成、破棄、インポートします。
Ansible Tower Inventory Reader	ファクト、ホスト、およびホストグループを表示します。
Bookmarks manager	ブックマークを作成、編集、削除します。
Boot disk access	起動ディスクをダウンロードします。
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、破棄を行い、コンプライアンスレポートを表示します。
Compliance viewer	コンプライアンスレポートを表示します。
Create ARF report	コンプライアンスレポートを作成します。
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。

ロール	ロールで提供されるパーミッション <a>[a]
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。
System admin	<ul style="list-style-type: none"> ● 管理 > 設定 でグローバル設定を編集します。 ● ユーザー、ユーザーグループ、ロールを参照、作成、編集、破棄します。 ● 組織とロケーションを参照、作成、編集、破棄、割り当てますが、その中のリソースは参照しません。 <p>このロールが割り当てられたユーザーは、ユーザーの作成や全ロールの割り当てが可能であるため、このロールは信頼できるユーザーにのみ割り当てるようにしてください。</p>
Tasks manager	Satellite タスクを表示および編集します。
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。
<p>[a] 事前定義されたロールに関連付けられた一連の許可済みアクションは、「ロールのパーミッションの表示」 で確認できます。</p>	

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ーであり、ほとんどのリソースタイプでサポートされています。

5.4.2. 詳細なパーミッションフィルターの作成

以下の手順を使用して、詳細なフィルターを作成します。

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。

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`

- `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。

CLI をご利用の場合

詳細なフィルターを作成するには、以下のように `--search` オプションを指定して `hammer filter create` を入力し、パーミッションフィルターで絞り込みます。

```
# hammer filter create \
--permission-ids 91 \
--search "name ~ ccv*" \
--role qa-user
```

このコマンドは、名前が `ccv` で始まるコンテンツビューのみを表示、作成、編集、破棄するパーミッションを `qa-user` ロールに追加します。

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

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

```
hostgroup = host-editors
```

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できるようにする場合には、**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5.1 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が必要です。
-----	-------------------------

表5.2 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ト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。サポート対象のプロファイルは、Red Hat Enterprise Linux の `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、デプロイ、変更、作成する方法については、『[Red Hat Enterprise Linux 7 セキュリティーガイド](#)』を参照してください。

Satellite 6 の OpenSCAP コンポーネントととも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 XCCDF 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



注記

ホストで OpenSCAP 監査を設定するために Puppet を使用しない場合は、この手順をスキップできます。

OpenSCAP でホストを監査するには、先に Puppet 環境をインポートする必要があります。Puppet 環境には、OpenSCAP 設定をデプロイするために各ホストに割り当てる必要のある Puppet クラスが含まれます。

Satellite Web UI で、Puppet 環境と、監査する各ホストを関連付ける必要があります。

手順

1. Satellite Web UI で、**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には、**実稼働** 環境のチェックボックスを選択します。OpenSCAP に必要な Puppet クラスは、デフォルトで **実稼働** 環境に含まれます。
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 Content**
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. コンプライアンスポリシーの作成

Satellite 6 では、ホストがセキュリティ要件に準拠するように、コンテンツホストをスキャンするコンプライアンスポリシーを作成できます。

Puppet または Ansible を使用して、ホストにコンプライアンスポリシーをデプロイできます。デフォルトでは Puppet は 30 分ごとに実行されます。新規ポリシーを割り当てる場合には、次の Puppet の実行でホストにポリシーを同期します。ただし、Ansible では、実行をスケジュールリングできません。リモート実行の詳細は、『**ホストの管理**』ガイドの「**リモートジョブの設定および実行**」を参照してください。

前提条件

開始する前に、Puppet または Ansible のどちらのデプロイメントを使用するかを決定する必要があります。

- Puppet デプロイメントの場合は、監査する各ホストが Puppet 環境に関連付けられていることを確認します。詳細は、「[OpenSCAP Puppet モジュールのインポート](#)」を参照してください。
- Ansible デプロイメントの場合は、**theforeman.foreman_scap_client** の Ansible ロールがインポートされていることを確認します。Ansible ロールのインポートに関する詳細は、[4章 Ansible ロールの管理](#)を参照してください。

手順

1. **ホスト > ポリシー** に移動して、手動、Ansible または Puppet のいずれかのデプロイメントを選択します。
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。

- 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。
[BZ#1704582](#) が解決されるまで、**Default XCCDF Profile** は空のレポートを返す可能性がある点に注意してください。
- 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 のリストから、**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** 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。
- 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。
- 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。
- 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ともに追加されます。**SCAP Content** 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. コンプライアンスポリシーの表示

特定の OpenSCAP コンテンツおよびプロファイルの組み合わせ別に適用されるルールをプレビューできます。これは、ポリシーを計画する場合に便利です。

Satellite Web UI で、コンプライアンスポリシーを表示します。

手順

- ホスト > ポリシー** に移動します。
- ガイドの表示** をクリックします。

6.3.4. コンプライアンスポリシーの編集

Satellite Web UI で、コンプライアンスポリシーを編集します。

手順

- ホスト > ポリシー** に移動します。
- 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。
- 必要な属性を編集します。
- 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. コンプライアンスポリシーの削除

Satellite Web UI で、既存のポリシーを削除します。

1. **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。

6.4. 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. OPENSAP 用のホストグループの設定

以下の手順を使用して、ホストグループに全 OpenSCAP 要件を設定します。

OpenSCAP 設定の概要

ホストグループに必要なコンポーネントを割り当てるには、Satellite Server で次のタスクを実行する必要があります。

- Capsule で OpenSCAP を有効にします。詳細は、『[Capsule Server のインストール](#)』ガイドの「[外部の Capsule での OpenSCAP の有効化](#)」を参照してください。
- OpenSCAP Capsule を割り当てます。
- OpenSCAP ポリシーをデプロイするための Puppet クラスを含む Puppet 環境を割り当ててます。
- **foreman_scap_client** および **foreman_scap_client::params** Puppet クラスを割り当てます。
- 追加するコンプライアンスポリシーを割り当てます。

ホストの作成および管理に関する詳細は、『[ホストの管理](#)』ガイドを参照してください。

手順

1. Satellite Web UI で **設定 > ホストグループ** に移動して、ホストグループを作成するか、OpenSCAP レポートを設定するホストグループをクリックします。
2. **Puppet 環境** リストから、**foreman_scap_client** および **foreman_scap_client::params** が含まれる Puppet 環境を選択します。
3. **OpenSCAP Capsule** リストから、使用する OpenSCAP が有効になった Capsule を選択します。
4. **Puppet クラス** タブをクリックして、**foreman_scap_client** と **foreman_scap_client::params** の Puppet クラスを追加します。
5. **送信** をクリックして変更を保存します。
6. **ホスト > ポリシー** に移動します。

7. ホストグループに割り当てるポリシーを選択します。
8. **ホストグループ** タブをクリックします。
9. **ホストグループ** リストから、このポリシーに割り当てるホストグループを任意の数だけ割り当てます。
10. **送信** をクリックして変更を保存します。

6.6. OPENSCAP のホスト設定

以下の手順を使用して、ホスト向けの OpenSCAP の全要件を設定します。

OpenSCAP 設定の概要

ホストに必要なコンポーネントを割り当てるには、Satellite Server で次のタスクを実行する必要があります。

- Capsule で OpenSCAP を有効にします。詳細は、『**Capsule Server のインストール**』ガイドの「**外部の Capsule での OpenSCAP の有効化**」を参照してください。
- OpenSCAP Capsule を割り当てます。
- OpenSCAP ポリシーをデプロイするための Puppet クラスを含む Puppet 環境を割り当ててます。
- **foreman_scap_client** および **foreman_scap_client::params** Puppet クラスを割り当てます。
- 追加するコンプライアンスポリシーを割り当てます。

ホストの作成および管理に関する詳細は、『**ホストの管理**』ガイドを参照してください。

手順

1. Satellite Web UI で **ホスト** > **すべてのホスト** に移動して、OpenSCAP レポートを設定するホストで、**編集** をクリックします。
2. **Puppet 環境** リストから、**foreman_scap_client** および **foreman_scap_client::params** が含まれる Puppet 環境を選択します。
3. **OpenSCAP Capsule** リストから、使用する OpenSCAP が有効になった Capsule を選択します。
4. **Puppet クラス** タブをクリックして、**foreman_scap_client** と **foreman_scap_client::params** の Puppet クラスを追加します。
5. コンプライアンスポリシーを追加するには、次のいずれかの場所に移動します。
6. **ホスト** > **すべてのホスト** に移動します。
7. ポリシーを追加するホストを選択します。
8. **アクションの選択** をクリックします。
9. 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。

10. ポリシーウィンドウで、利用可能なポリシーの一覧からポリシーを選択して、**送信** をクリックします。

6.7. コンプライアンスの監視

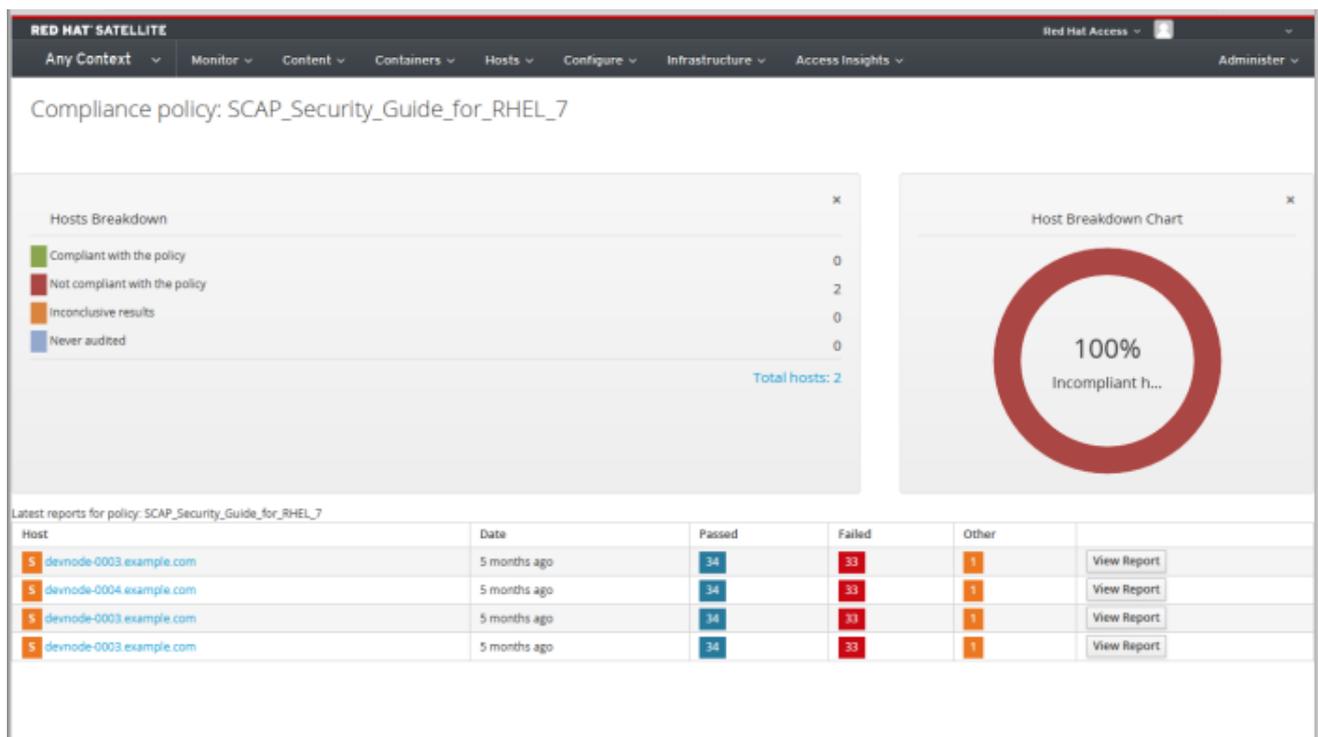
Red Hat Satellite 6 では、コンプライアンスを一元化して監視および管理できます。コンプライアンスダッシュボードには、ホストのコンプライアンスの概要が表示され、そのポリシーの範囲内にある各ホストの詳細を表示する機能が提供されます。コンプライアンスレポートでは、適用可能なポリシーを使用して、各ホストのコンプライアンスの詳細を分析します。この情報を使用して、各ホストが提示するリスクを評価し、ホストがコンプライアンスを満たすために必要なリソースを管理できます。

SCAP を使用してコンプライアンスを監視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

6.7.1. 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では、ホストのコンプライアンスの統計的なサマリーが表示され、そのポリシーの範囲内にある各ホストの詳細を表示できます。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** の統計から、コンプライアンスタスクの優先付けに便利なメトリクスが提供されます。**Never audited** として検出されたホストも、ステータスが不明なため、優先する必要があります。



6.7.2. コンプライアンスポリシーダッシュボードの表示

Satellite Web UI を使用して、コンプライアンスポリシーダッシュボードでポリシーコンプライアンスを検証します。

手順

1. Satellite Web UI で、**ホスト > ポリシー** に移動します。

2. 必要なポリシー名をクリックします。ダッシュボードに次の情報が提供されます。
 - ホストのポリシーコンプライアンスの状況を概要ビューで表示するリングチャート。
 - ホストのポリシーに関する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

6.7.3. コンプライアンスのメール通知

Satellite Server は、**Openscap ポリシーサマリー** 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 サマリー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、各ポリシーのサマリーと直近の結果を提供します。

OpenSCAP サマリー 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。

6.7.4. コンプライアンスレポート

コンプライアンスレポートには、ホストに対するポリシー実行の結果が出力されます。各レポートには、ポリシーごとの合格または不合格の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にリストされます。

Satellite Web UI で、**ホスト > レポート** に移動して、すべてのコンプライアンスレポートを一覧表示します。

コンプライアンスレポートは以下のエリアで構成されます。

- Introduction (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)

Evaluation Characteristics (評価特性)

Evaluation Characteristics (評価特性) エリアでは、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。

名前	説明	例
Target machine	評価対象ホストの完全修飾ドメイン名 (FQDN)。	test-system.example.com

名前	説明	例
Benchmark URL	ホストが評価された SCAP コンテンツの URL。	<code>/var/lib/openscap/content/1fbdc87d24db51ca184419a2b6f</code>
Benchmark ID	ホストが評価されたベンチマークの識別子。ベンチマークは、プロファイルのセットです。	<code>xccdf_org.ssgproject.content_benchmark_RHEL_7</code>
Profile ID	ホストが評価されたプロファイルの識別子。	<code>xccdf_org.ssgproject_content_profile_rht-ccp</code>
Started at	評価の開始日時 (ISO 8601 形式)。	<code>2015-09-12T14:40:02</code>
Finished at	評価の終了日時 (ISO 8601 形式)。	<code>2015-09-12T14:40:05</code>
Performed by	ホストで評価を実行したローカルアカウントの名前。	<code>root</code>

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

Compliance and Scoring (コンプライアンスおよびスコアリング) エリアでは、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** フィールドで **その他** として分類されます。

Rule Overview (ルールの概要)

Rule Overview (ルールの概要) エリアでは、階層的なレイアウトで示されるルールと、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。

6.7.5. ホストのコンプライアンス違反の調査

Satellite Web UI を使用して、ホストがルールのコンプライアンス違反をした理由を特定します。

手順

1. Satellite Web UI で、**ホスト > レポート** に移動して、すべてのコンプライアンスレポートを一覧表示します。

2. 個々のレポートの詳細を表示するには、特定のホストの行で **レポートの表示** をクリックします。
3. 詳細を確認するには、ルールタイトルをクリックします。
 - ルールの説明。可能な場合は、ホストがコンプライアンスを満たすための指示を含みません。
 - ルールの根拠。
 - 場合により、修復スクリプト。



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。

6.7.6. 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、任意のホストのサブセットに関して入手可能なレポート一覧を絞り込みます。

手順

- フィルターを適用するには、**検索** フィールドに検索クエリーを入力し、**検索** をクリックします。検索クエリーでは大文字と小文字は区別されません。

ユースケースの検索

- 以下の検索クエリーでは、6つ以上のルールに合格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
```

- 以下の検索クエリーでは、ホスト名に **prod-** の文字が含まれるホストで、YYYY年1月1日より後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 > "Jan 1, YYYY"
```

- 以下の検索クエリーでは、**rhel7_audit** コンプライアンスポリシーを使用して、1時間前以降に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
```

- 以下の検索クエリーでは、XCCDF ルールに合格のレポートが検索されます。

```
xccdf_rule_passed = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

- 以下の検索クエリーは、XCCDF ルールに不合格のレポートが検索されます。

```
xccdf_rule_failed = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

- 以下の検索クエリーは、結果が XCCDF ルールに合格または不合格以外のレポートが検索されます。

```
xccdf_rule_othered = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

追加情報

- 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ー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。
- 正規表現は検索クエリーで使用できませんが、単一の検索式に複数のフィールドを使用できます。利用可能なすべての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。
- 検索をブックマークすると、同じ検索クエリーを再利用できます。詳細は「[ブックマークの作成](#)」を参照してください。

6.7.7. コンプライアンスレポートの削除

コンプライアンスレポートを削除するには、次の手順を実行します。

1. Satellite Web UI で、**ホスト > レポート** に移動します。
2. コンプライアンスレポートウィンドウで、削除するポリシーを特定し、ポリシーの名前の右側にある **削除** を選択します。
3. **OK** をクリックします。

6.7.8. 複数のコンプライアンスレポートの削除

複数のコンプライアンスポリシーを同時に削除できます。ただし、Satellite Web UI では、コンプライアンスポリシーはページ分割されているため、レポートを1ページずつ削除する必要があります。すべての OpenSCAP レポートを削除する場合は、『[Red Hat Satellite API ガイド](#)』の「[OpenSCAP レポートの削除](#)」セクションのスクリプトを使用します。

1. Satellite Web UI で、**ホスト > レポート** に移動します。
2. コンプライアンスレポートウィンドウで、削除するコンプライアンスレポートを選択します。
3. リストの右上の **レポートの削除** を選択します。
4. 削除するページ数だけ、この手順を繰り返します。

6.8. OPENSAP 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 強度の低い暗号化の無効化

インフラストラクチャーのセキュリティー要件に応じて、Satellite の暗号化設定を変更したり、脆弱性を素早く修正したりする場合があります。以降のセクションを使用して、強度の低い SSL 暗号化と 64 ビットの暗号スイートを無効にします。

7.1. 強度の低い SSL 2.0 および SSL 3.0 暗号化の無効化

Satellite が SSL の脆弱性が原因で Nessus スキャンを失敗した場合、またはセキュリティーインフラストラクチャーで SSL 2.0 と SSL 3.0 の無効化が必要な場合には、`/etc/foreman-installer/custom-hiera.yaml` ファイルを編集して、強度の低い暗号化を削除できます。

Satellite の強度の低い SSL 2.0 および SSL 3.0 暗号化を無効にする手順

Satellite で強度の低い暗号化を無効にするには、次の手順を実行します。

1. `/etc/foreman-installer/custom-hiera.yaml` ファイルを開いて、編集します。

```
# vi /etc/foreman-installer/custom-hiera.yaml
```

2. 次のエントリーを追加します。

```
# Foreman Proxy
foreman_proxy::tls_disabled_versions: ['1.1']

# Dynflow
foreman_proxy::plugin::dynflow::tls_disabled_versions: ['1.1']

# Apache
apache::mod::ssl::ssl_protocol: ['ALL', '-SSLv3', '-TLSv1', '-TLSv1.1', '+TLSv1.2']

# Tomcat / Candlepin
candlepin::tls_versions: ['1.2']

# QPID Dispatch
foreman_proxy_content::qpid_router_ssl_protocols: ['TLSv1.2']
foreman_proxy_content::qpid_router_ssl_ciphers: 'ALL:!aNULL:+HIGH:-SSLv3:!IDEA-CBC-SHA'
```

3. `satellite-installer` ツールを引数なしで再実行します。

```
# satellite-installer
```

4. `satellite-maintain` サービスを再起動します。

```
# satellite-maintain service restart
```

Capsule の強度の低い SSL 2.0 および SSL 3.0 暗号化を無効にする手順

Capsule の強度の低い暗号化を無効にするには、次の手順を実行します。

1. `/etc/foreman-installer/custom-hiera.yaml` ファイルを開いて、編集します。

```
# vi /etc/foreman-installer/custom-hiera.yaml
```

2. 次のエントリーを追加します。

```
# Foreman Proxy
foreman_proxy::tls_disabled_versions: ['1.1']

# Dynflow
foreman_proxy::plugin::dynflow::tls_disabled_versions: ['1.1']

# Apache
apache::mod::ssl::ssl_protocol: ['ALL', '-SSLv3', '-TLSv1', '-TLSv1.1', '+TLSv1.2']

# QPID Dispatch
foreman_proxy_content::qpid_router_ssl_protocols: ['TLSv1.2']
foreman_proxy_content::qpid_router_ssl_ciphers: 'ALL:!aNULL:+HIGH:-SSLv3:!IDEA-CBC-SHA'

# PULP
pulp::ssl_protocol: "ALL -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2"
```

3. **satellite-installer** ツールを引数なしで再実行します。

```
# satellite-installer
```

4. **satellite-maintain** サービスを再起動します。

```
# satellite-maintain service restart
```

7.2. 64 ビットブロックサイズ暗号スイート (SWEET32) の無効化

Satellite の暗号スイートを更新する場合は、暗号を編集してから、**/etc/foreman-installer/custom-hiera.yaml** ファイルに変更を加え、これらの変更を永続化します。

暗号スイートを更新するには、次の手順を使用できます。

[BZ#1586271](#) が解決されるまで、SSL 64 ビットブロックサイズ暗号スイート (SWEET32) を無効にすることをお勧めします。ただし、以下の手順を使用して、他の暗号を更新し、これらの変更を永続化することもできます。

以下の暗号のブラウザー最小要件は、Firefox 27 です。

1. **/etc/httpd/conf.d/ssl.conf** Apache 設定ファイルを開いて、編集します。

```
# vi /etc/httpd/conf.d/ssl.conf
```

2. **SSLCipherSuite** パラメーターの値を更新します。

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
```

3. **httpd** サービスを再起動します。

```
# systemctl restart httpd
```

- 別の `satellite-installer` 実行で変更を永続化するには、`/etc/foreman-installer/custom-hiera.yaml` ファイルを開いて、編集します。

```
# vi /etc/foreman-installer/custom-hiera.yaml
```

- `apache` の次のエントリーを追加します。

```
apache::mod::ssl::ssl_cipher: ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-  
AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-  
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-  
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-  
ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
```

- `satellite-installer` ツールを実行して、Apache の設定を変更します。

```
# satellite-installer -S satellite
```

第8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。

8.1. SATELLITE のバックアップ

Satellite Server または Capsule Server のバックアップは、Satellite または Capsule の復元またはデバッグに使用できるアーカイブされたデータベースと設定ファイルの集まりです。**satellite-maintain backup** ユーティリティを使用して、バックアップを作成します。

バックアップの種類

次の種類のバックアップを作成できます。

完全

Satellite または Capsule の完全なバックアップ。

増分

前回のバックアップ以降の変更のバックアップ。

Pulp コンテンツなし

Pulp データベースコンテンツを含まない部分バックアップ。

バックアップの方法

バックアップの実行には、次の方法を使用できます。

オフライン

オフラインで Satellite または Capsule のバックアップを作成します。

オンライン

オンラインで Satellite または Capsule のバックアップを作成します。

スナップショット

論理ボリュームマネージャー (LVM) のスナップショットからバックアップを作成します。Satellite または Capsule は、スナップショットの作成中はオフラインです。

バックアップの方法と種類の詳細は、[「バックアップの方法と種類」](#)を参照してください。

satellite-maintain backup ユーティリティを使用すると、指定したディレクトリーにサブディレクトリーに、タイムスタンプ付きでバックアップが作成されます。**--preserve-directory** オプションを使用して、サブディレクトリーに別の名前を指定できます。**--preserve-directory** オプションを使用すると、バックアップの失敗時には、サブディレクトリーは消去されません。

Satellite または Capsule がリモートデータベースを使用するように設定されている場合には、オフラインまたはスナップショットバックアップの実行時に、このユーティリティでデータベースダンプが実行されます。

バックアップの考慮事項

- バックアップは定期的を作成してください。cron ジョブを使用した定期的バックアップのスケジュール設定の詳細は、「[オフラインバックアップのスケジュール設定のスク립ト例](#)」を参照してください。
- バックアップの安全性を確保するには、別のシステム上の別のストレージにバックアップを作成します。
- バックアップには、`/root/ssl-build` ディレクトリーの機密情報が含まれます。たとえば、ホスト名、SSH キー、要求ファイル、SSL 証明書が含まれる場合があります。バックアップを暗号化するか、安全な場所に移動し、破損のリスクやホストへの不正アクセスを最小限に抑えます。

8.2. 完全バックアップ

Satellite または Capsule Server の完全バックアップには、Satellite または Capsule のインスタンスの復元に必要なすべてのデータベースと設定ファイルが含まれます。

バックアップのコンテンツ

完全バックアップには、以下のファイルが含まれます。

- 圧縮された設定ファイル
- 圧縮された MongoDB ファイル
- 圧縮された PostgreSQL データベースファイル
- Pulp ディレクトリーファイル
- Satellite 環境の詳細を含む設定ファイル

ストレージ要件

完全バックアップでは、ファイルのコピー後に圧縮されるので、(コピーしたファイルと圧縮ファイルの) 両方を保持する十分なストレージが必要です。さらに、アーカイブと圧縮時に作成されるメタデータファイル用に、追加のスペースが必要です。

Satellite または Capsule の完全バックアップでは、以下を合計した値のストレージ量が必要です。

- Satellite データベースおよび設定ファイルのサイズ
- 圧縮された Satellite データベースおよび設定ファイルのサイズ
- 圧縮前および圧縮後のデータベースおよび設定ファイルのサイズの合計の 20%

8.2.1. 完全バックアップサイズの見積もり

バックアップサイズを見積もるには、データベースと設定ファイルで使用する容量の合計を検索します。この結果を使用して、バックアップサイズを計算します。

手順

1. `du` コマンドを使用して、データベースおよび設定ファイルのサイズを検索します。

```
# du -csh /var/lib/mongodb /var/lib/pgsql/data /var/lib/pulp /var/lib/qpidd /var/lib/tftpboot /etc
/root/ssl-build /var/www/html/pub /opt/puppetlabs
```

例:

```
# du -csh /var/lib/mongodb /var/lib/pgsql/data /var/lib/pulp /var/lib/qpidd /var/lib/tftpboot /etc
/root/ssl-build /var/www/html/pub /opt/puppetlabs
480G /var/lib/mongodb
100G /var/lib/pgsql/data
100G /var/lib/pulp
886M /var/lib/qpidd
16M /var/lib/tftpboot
37M /etc
900K /root/ssl-build
100K /var/www/html/pub
2M /opt/puppetlabs
681G total
```

この例では、ファイルのサイズは 681 GB です。

2. 上記の結果を使用して、圧縮データの保存に必要な容量を計算します。
圧縮データのサイズを見積もる方法の詳細は、「[バックアップデータ圧縮率](#)」を参照してください。

この例では、バックアップの圧縮データに 180 GB が必要です。

3. 必要な追加の空き容量を計算します。
必要な追加容量は、圧縮後および圧縮前のファイルの合計の 20% であるため、この例で必要な追加容量は 178 GB です。
4. 上記の結果の合計を計算します。
この例では、次のようになります。

```
Uncompressed size = 861 GB
Compressed size = 180 GB
Additional free space required = 172 GB
Sum = 1033 GB
```

この例では、バックアップの見積もりサイズは 1033 GB です。

8.2.2. 完全バックアップのオフライン実行

オフライン方法を使用して完全バックアップを実行します。バックアッププロセスが完了するまでの所要時間は長く、Satellite はこのバックアップ処理中は使用できません。

前提条件

- バックアップ場所には、バックアップを保存するのに十分な空きディスク領域がある。詳細については、「[完全バックアップサイズの見積もり](#)」を参照してください。
- **postgres** ユーザーに、バックアップディレクトリーへの書き込み権限が割り当てられている。

手順

1. **satellite-maintain backup** スクリプトを実行します。

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

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

バックアッププロセスの完了までに長時間かかります。

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、[「バックアップユーティリティーの追加オプション」](#) を参照してください。

8.2.3. 完全バックアップのオンライン実行

問題をデバッグし、トラブルシューティングを行うには、オンライン方法を使用して、完全バックアップを実行します。Satellite はバックアップ処理中でも使用できます。

バックアップを成功させるには、バックアップが完了するまで次の操作を実行しないでください。

- コンテンツビューの公開、追加、または削除
- コンテンツビューバージョンのプロモート
- 同期プランの追加、変更、または削除
- リポジトリの追加、削除、または同期

バックアッププロセスの完了までに長時間かかります。

前提条件

- バックアップ場所には、バックアップを保存するのに十分な空きディスク領域がある。詳細については、[「完全バックアップサイズの見積もり」](#) を参照してください。
- **postgres** ユーザーに、バックアップディレクトリーへの書き込み権限が割り当てられている。

手順

1. **satellite-maintain backup** スクリプトを実行します。

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

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

バックアッププロセスの完了までに長時間かかります。

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、[「バックアップユーティリティーの追加オプション」](#) を参照してください。

8.3. 増分バックアップ

増分バックアップには、前回実行したバックアップ以降に、データベースと設定ファイルに加えられた変更が含まれます。

最初の増分バックアップは完全バックアップをベースとし、その後の増分バックアップは前回のバックアップをベースとします。増分バックアップを使用して Satellite を復元するには、すべての増分バックアップと最初の完全バックアップが必要です。

8.3.1. 増分バックアップのオフライン実行

オフライン方法を使用して、増分バックアップを実行します。Satellite は、バックアップ処理中は使用できません。

前提条件

- 増分バックアップのベースとして使用する前回のバックアップが利用可能であること。
- **postgres** ユーザーに、バックアップディレクトリーへの書き込み権限が割り当てられている。

手順

1. **satellite-maintain backup** スクリプトを実行します。

```
# satellite-maintain backup offline --incremental /var/backup_dir/previous_backup_dir
/var/backup_dir
```

previous_backup_dir を、増分バックアップのベースとして使用する前回のバックアップの名前に置き換えます。

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、[「バックアップユーティリティーの追加オプション」](#) を参照してください。

8.3.2. 増分バックアップのオンライン実行

問題をデバッグし、トラブルシューティングを行うには、オンライン方法を使用して、増分バックアップを実行します。Satellite は、バックアップ処理中でも使用できます。

バックアップを成功させるには、バックアップが完了するまで次の操作を実行しないでください。

- コンテンツビューの公開、追加、または削除
- コンテンツビューバージョンのプロモート
- 同期プランの追加、変更、または削除

- リポジトリの追加、削除、または同期

前提条件

- 増分バックアップのベースとして使用する前回のバックアップが利用可能であること。
- **postgres** ユーザーに、バックアップディレクトリーへの書き込み権限が割り当てられている。

手順

1. **satellite-maintain backup** スクリプトを実行します。

```
# satellite-maintain backup online --incremental /var/backup_dir/previous_backup_dir
/var/backup_dir
```

previous_backup_dir を、増分バックアップのベースとして使用する前回のバックアップの名前に置き換えます。

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、「[バックアップユーティリティーの追加オプション](#)」を参照してください。

8.4. PULP コンテンツを含まないバックアップ

Pulp コンテンツを含まないバックアップでは、Satellite または Capsule Server のリポジトリ情報が除外されます。Pulp データベースに含まれるリポジトリ情報のバックアップは、Satellite バックアッププロセスで最も時間のかかる部分です。**--skip-pulp-content** オプションを使用して、Pulp データベースのバックアップをスキップできます。このオプションを使用すると、**/var/lib/pulp** ディレクトリーのバックアップが除外されます。

Pulp コンテンツを含まないバックアップから復元することはできません。

8.4.1. Pulp コンテンツを含まないバックアップのオフライン実行

問題をデバッグし、トラブルシューティングを行うには、オフライン方法を使用して、Pulp コンテンツを含まないバックアップを実行します。Satellite は、バックアップ処理中は使用できません。

手順

1. **satellite-maintain backup** スクリプトを実行します。

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

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

rsync や共有ストレージなどの方法を使用して、**/var/lib/pulp** の内容をコピーできます。

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、[「バックアップユーティリティーの追加オプション」](#) を参照してください。

8.4.2. Pulp コンテンツを含まないバックアップのオンライン実行

問題をデバッグしてトラブルシューティングするには、オンライン方法を使用して、Pulp コンテンツを含まないバックアップを作成します。Satellite は、バックアップ処理中でも使用できます。

手順

1. **satellite-maintain backup** スクリプトを実行します。

```
# satellite-maintain backup online --skip-pulp-content /var/backup_directory
```

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

rsync や共有ストレージなどの方法を使用して、**/var/lib/pulp** の内容をコピーできます。

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、[「バックアップユーティリティーの追加オプション」](#) を参照してください。

8.5. スナップショットのバックアップ

スナップショットのバックアップ方法は、Pulp、MongoDB、および PostgreSQL データベース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作成して、別の論理ボリューム (LV) にマウントします。

satellite-maintain backup ユーティリティーは、Satellite サービスがアクティブな時にスナップショットを作成し、バックアップに影響のあるサービスのみを停止します。Satellite または Capsule は、スナップショットを作成する場合のみ使用できません。バックアップが成功すると、すべてのサービスが再起動され、LVM スナップショットは削除されます。スナップショットのバックアップは、オフラインでの完全バックアップよりも所要時間が短く、Satellite または Capsule のダウンタイムが短縮されます。

8.5.1. スナップショットバックアップの実行

スナップショットの方法を使用してバックアップを実行します。Satellite は、LVM スナップショットを作成する場合には使用できません。

前提条件

- システムで、以下のディレクトリーに対して LVM が使用されていること。
 - **/var/lib/pulp/**
 - **/var/lib/mongodb/**
 - **/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。

手順

1. **satellite-maintain backup** スクリプトを実行します。

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

2. バックアップを開始するようにプロンプトが表示されたら、**y** を入力します。

```
Do you want to proceed?, [y(yes), q(quit)] y
```

リンク

- 追加の **satellite-maintain backup** ユーティリティーオプションのリストについては、「[バックアップユーティリティーの追加オプション](#)」を参照してください。

8.6. 従来のバックアップ

Red Hat Enterprise Linux システムの従来のバックアップとリカバリーの方法を使用して、Satellite または Capsule Server をバックアップすることもできます。

従来のバックアップを実行する前に、**satellite-maintain service stop** コマンドを使用して Satellite サービスを停止し、完了後に **satellite-maintain service start** コマンドを使用してサービスを再起動します。

詳細は、『Red Hat Enterprise Linux 7 システム管理者のガイド』の「[システムバックアップおよびリカバリー](#)」セクションを参照してください。

8.7. バックアップデータ圧縮率

次の表は、Satellite データベースのデータ圧縮率を示しています。

表8.1 データと圧縮率

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

データ型	ディレクトリー	比率	圧縮結果の例
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

8.8. バックアップユーティリティーの追加オプション

次の表で、**satellite-maintain backup** ユーティリティーで提供される追加オプションについてまとめています。

表8.2 バックアップの追加オプション

オプション	用途	例
--assumeeyes	確認プロンプトをスキップ。	satellite-maintain backup offline --assumeeyes
--whitelist	バックアップのラベル付きのステップをスキップ。ステップラベルのリストを表示するには、 satellite-maintain advanced procedure run -h コマンドを実行します。	satellite-maintain backup offline --whitelist backup-metadata -y /var/backup_directory
--preserve-directory	バックアップにカスタム名を指定。	satellite-maintain backup offline --preserve-directory /var/backup_directory/ first-backup

8.9. オフラインバックアップのスケジュール設定のスク립ト例

完全バックアップとその後の日次増分バックアップの設定

以下のスク립トでは、日曜日に完全バックアップを実行した後に、増分バックアップを毎日実行します。バックアップが実行されるたびに、新しいサブディレクトリーが作成されます。このスク립トでは、日次の cron ジョブが必要になります。

satellite-maintain backup スクリプトでは、**PATH** に **/sbin** と **/usr/sbin** のディレクトリーを指定する必要があります。

```
#!/bin/bash -e
PATH=/sbin:/bin:/usr/sbin:/usr/bin
DESTINATION=/var/backup_directory
if [[ $(date +%w) == 0 ]]; then
  satellite-maintain backup offline --assumeeyes $DESTINATION
```

```

else
  LAST=$(ls -td -- $DESTINATION/*/ | head -n 1)
  satellite-maintain backup offline --assumeeyes --incremental "$LAST" $DESTINATION
fi
exit 0

```

8.10. バックアップの方法と種類

次の表では、Satellite バックアップの種類と方法についてまとめています。

表8.3 バックアップの方法と種類

バックアップ	種類	方法	コマンド
復元	完全、増分	オフライン	satellite-maintain backup offline [--incremental]
	-	スナップショット	satellite-maintain snapshot
デバッグ	Pulp コンテンツなし	オフライン	satellite-maintain backup offline --skip-pulp-content
	完全、増分、Pulp コンテンツなし	オンライン	satellite-maintain backup online [--incremental][--skip-pulp-content]

第9章 バックアップからの SATELLITE SERVER または CAPSULE SERVER の復元

「[Satellite 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 を復元できます。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を復元する方法を概説します。バックアップに含まれる全データはターゲットシステムで削除されます。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をプロビジョニングしてください。

9.1. 完全バックアップからの復元

以下の手順を使用して、完全バックアップから Red Hat Satellite または Capsule Server を復元します。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。

前提条件

- 適切なインスタンスに復元していること。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。
- 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する。
ディレクトリーの使用量を確認するには、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。

- すべての SELinux コンテキストが適切であることを確認する。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 /
```

手順

- Satellite または Capsule 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。

```
# satellite-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が原因で、復元プロセスの完了には時間がかかることがあります。

リンク

- 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。

9.2. 増分バックアップからの復元

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するブランチの各増分バックアップを時系列で選択します。

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。

手順

1. 「完全バックアップからの復元」の手順を使用して、最新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。

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

`satellite-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、このコマンドに `-i` オプションを使用する必要はありません。

リンク

- 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。

9.3. 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、-certs.tar で終わるパッケージ名で、Satellite Server にもまだ残っている可能性があります。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、「[外部 Capsule からの同期](#)」の手順で Satellite から同期します。

9.3.1. 外部 Capsule からの同期

外部 Capsule と Satellite を同期します。

手順

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)** 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10章 SATELLITE SERVER または CAPSULE SERVER の名前の変更

Satellite Server または Capsule Server の名前を変更するには、**satellite-change-hostname** スクリプトを使用する必要があります。

Satellite Server の名前を変更する場合は、すべてのSatellite クライアントを再登録し、新しい Satellite ホスト名を指すように各 Capsule Server を設定する必要があります。カスタム SSL 証明書を使用する場合は、新しいホスト名で再生成する必要があります。

Capsule Server の名前を変更する場合は、すべての Capsule クライアントを再登録し、Satellite Web UI で Capsule ホスト名を更新する必要があります。カスタム SSL 証明書を使用する場合は、新しいホスト名で再生成する必要があります。



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。

10.1. SATELLITE SERVER の名前の変更

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 に登録されているホストが通信用に使用しています。この手順により、すべての参照を新しいホスト名に確実に更新することができます。

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、[13章 外部認証の設定](#) を参照してください。

前提条件

- Satellite Server をバックアップすること。**satellite-change-hostname** スクリプトを実行すると、Satellite Server への変更は元に戻せません。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。
- オプション: Satellite Server がカスタムの SSL 証明書をインストールしている場合は、ホストの新しい名前用に新しい証明書を取得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「[カスタムの SSL 証明書を使用した Satellite Server の設定](#)」を参照してください。

手順

1. Satellite Server で **satellite-change-hostname** スクリプトを実行する適切な方法を選択して、新しいホスト名と Satellite 認証情報を提供します。
 - Satellite Server をデフォルトの自己署名 SSL 証明書でインストールした場合は、以下のコマンドを入力します。

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

- Satellite Server をカスタムの 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 \  
--custom-cert "/root/ownca/test.com/test.com.crt" \  
--custom-key "/root/ownca/test.com/test.com.key"
```

2. オプション: Satellite Server の新しいホスト名用にカスタム SSL 証明書を作成した場合は、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 SSL 証明書のインストールに関する詳細は、『[オンラインネットワークからの Satellite Server のインストール](#)』の「[カスタムの SSL 証明書の Satellite Server へのデプロイ](#)」を参照してください。
3. すべての Satellite クライアントで以下のコマンドを入力して、ブートストラップ RPM を再インストールし、クライアントを再登録して、サブスクリプションを更新します。この手順は、リモート実行機能を使用して実行できます。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。

```
# yum remove -y katello-ca-consumer*  
  
# rpm -Uvh http://new-satellite.example.com/pub/katello-ca-consumer-latest.noarch.rpm  
  
# subscription-manager register \  
--org="Default_Organization" \  
--environment="Library" \  
--force  
  
# subscription-manager refresh
```

4. すべての Capsule Server で、Satellite インストールスクリプトを実行して、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
```

5. Satellite Server で、すべての Capsule Server を一覧表示します。

```
# hammer capsule list
```

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

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

10.2. CAPSULE SERVER の名前の変更

Capsule Server のホスト名は、Satellite Server のコンポーネントおよび Capsule Server に登録されている全ホストが参照しています。この手順により、新規ホスト名への参照をすべて更新することができます。

前提条件

- Capsule Server をバックアップすること。**satellite-change-hostname** スクリプトを実行すると、Capsule Server への変更は元に戻せません。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、[8章 Satellite Server および Capsule Server のバックアップ](#) を参照してください。

手順

1. Satellite Server で、Capsule Server の新しい証明書のアーカイブファイルを生成します。

- デフォルトの SSL 証明書を使用している場合は、以下のコマンドを実行します。

```
# capsule-certs-generate \  
--foreman-proxy-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。

- カスタムの SSL 証明書を使用している場合は、Capsule Server 用の新しい SSL 証明書を作成します。詳細は、『[Installing Capsule Server](#)』の「[Configuring Capsule Server with a Custom SSL Certificate](#)」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。

4. オプション: Capsule Server で、Capsule Server のカスタム証明書を作成した場合、証明書をデプロイするには、**capsule-certs-generate** コマンドが返す **satellite-installer** コマンドを入力します。詳細は、『[Capsule Server のインストール](#)』の「[カスタムの SSL 証明書の Capsule Server へのデプロイ](#)」を参照してください。
5. すべての Capsule クライアントで、以下のコマンドを入力して、ブートストラップ RPM を再インストールし、クライアントを再登録して、サブスクリプションを更新します。この手順は、リモート実行機能を使用して実行できます。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。

```
# 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

# subscription-manager refresh
```

6. Satellite Web UI で、**インフラストラクチャー > Capsules (スマートプロキシ)** に移動します。
7. リストで Capsule Server を見つけ、右側にある **編集** をクリックします。
8. **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。
9. 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11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、未使用タスクの消去方法、いっぱいになったディスクから Pulp を復元する方法、MongoDB からディスク領域を解放する方法などの Red Hat Satellite Server のメンテナンス方法について説明します。

11.1. 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、監査はいつでも取り消すことができます。また、cron ジョブを使用して、設定した間隔で、監査レコードの削除をスケジューリングすることも可能です。

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して、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
```

11.2. 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 ジョブを使用して、設定した間隔で、監査レコードの削除をスケジューリングすることも可能です。

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して、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
```

11.3. 未使用タスクのクリーニング機能の設定

Satellite はクリーニングを定期的に行うことで、データベース内のディスク領域を削減し、ディスク増加率を制限します。その結果、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向上します。

デフォルトでは、Satellite は毎日 19 時 45 分にタスクをクリーンアップする cron ジョブを実行します。Satellite は、クリーニング中に以下のタスクを削除します。

- 正常に実行され、30日を超過したタスク
- 1年を超過したすべてのタスク

以前のバージョンからアップグレードされた Satellite の場合

[BZ#1788615](#) が解決されるまで、この機能は Satellite 6.6 以降の新規インストールでのみ機能します。以前のバージョンから Satellite をアップグレードすると、この機能はデフォルトで無効になります。Satellite が定期的なクリーニングを実行できるようにするには、以下のコマンドを入力します。

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

オプションでこの手順を使用して設定を調整し、ニーズに対応します。

手順

1. オプション: Satellite が cron ジョブを実行する時刻を設定するには、**--foreman-plugin-tasks-cron-line** パラメーターを cron 形式で希望する時刻に設定します。たとえば、cron ジョブを毎日 15 時 00 分に実行するようにスケジュールするには、以下のコマンドを入力します。

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

2. オプション: Satellite がタスクを削除するまでの期間を設定するには、**/etc/foreman/plugins/foreman-tasks.yaml** ファイルの **:rules:** セクションを編集します。

11.4. 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) に空き領域がない場合の解決方法について説明します。

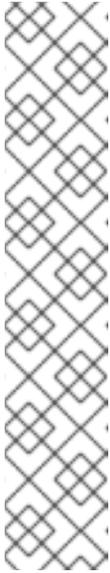
完全なディスクからのリカバリー方法

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 に十分な空き領域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、多くの領域が解放されるわけではありません。

- b. できるだけ多くのレ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、『[Red Hat Enterprise Linux 7 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-maintain** サービスを停止します。

```
# satellite-maintain service stop
```

- LV 上のファイルシステムを拡張します。

- **satellite-maintain** サービスを起動します。

```
# satellite-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。

11.5. 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。バックアップの作成手順については、「[完全バックアップのオフライン実行](#)」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 からディスク領域を確保する方法

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。

- 修復後の MongoDB のディスク領域の使用量を確認します。

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

- Pulp サービスを開始します。

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

11.6. SATELLITE SERVER のベースオペレーティングシステムでのパッケージの管理

Satellite のベースオペレーティングシステムでパッケージをインストールして更新するには、**satellite-maintain packages** コマンドを入力する必要があります。

Satellite は、**yum** を使用したパッケージのインストールと更新はできません。理由は、**yum** は、Satellite 関連のパッケージを更新し、システムの不整合が発生する可能性があるためです。



重要

Satellite Server で、パッケージのインストール後に **satellite-installer --upgrade** コマンドが実行されるため、**satellite-maintain packages** コマンドは Satellite Server のサービスの一部を再起動します。

手順

- Satellite Server でパッケージをインストールするには、以下のコマンドを入力します。

```
# satellite-maintain packages install package_1 package_2
```

- Satellite Server でパッケージを更新するには、以下のコマンドを入力します。

```
# satellite-maintain packages update package_1 package_2
```

yum を使用したパッケージ更新の確認

yum を使用して更新を確認する場合は、コマンドを入力して手動でパッケージをインストールおよび更新してから、**yum** を使用して更新を確認できます。

```
# satellite-maintain packages unlock
# yum check update
# satellite-maintain packages lock
```

パッケージを個別に更新すると、Satellite でパッケージの不整合が発生する可能性があります。Satellite でのパッケージの更新の詳細については、[Satellite Server のアップデート](#) を参照してください。

Satellite のパッケージ管理での yum の有効化

yum を使用して直接システムにパッケージをインストールして更新し、システムの安定性をご自身で管理する場合は、以下のコマンドを入力します。

```
# satellite-maintain packages unlock
```

パッケージ管理のデフォルト設定への復元

デフォルト設定を復元し、Satellite を有効にしてユーザーが **yum** を使用してパッケージをインストールおよび更新できないようにし、システムの安定性を確保する必要がある場合は、以下のコマンドを入力します。

```
# satellite-maintain packages lock
```

第12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。

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。

Satellite のロギング設定の詳細は、**satellite-installer** を使用し、**--full-help** オプションを指定します。

```
# satellite-installer --full-help | grep logging
```

12.1. デバッグロギングの有効化

デバッグロギングでは、最も詳細にわたるログ情報が提供され、Satellite 6.6 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。

Satellite CLI で、デバッグロギングを有効にして、Satellite 6.6 の詳細なデバッグ情報をログに記録します。

手順

デバッグロギングを有効にするには、Satellite Server で次の手順を実行します。

1. デバッグロギングを有効にするには、次のコマンドを入力します。

```
# satellite-installer --foreman-logging-level debug
```

2. デバッグが完了したら、ロギングレベルをデフォルト値にリセットします。

```
# satellite-installer --reset-foreman-logging-level
```

12.2. 個別のロガーの有効化

個別のロガーを有効にして、一部のロギングを選択的に有効にできます。Satellite では、以下のロガーを使用します。

app

Web 要求とアプリケーションの一般的なメッセージをすべてロギングします。デフォルト値: true

audit

追加のファクト統計、追加、更新、削除されたファクトの数をロギングします。デフォルト値: true

ldap

ハイレベルの LDAP クエリーと LDAP オペレーションをロギングします。デフォルト値: false

permissions

ページを読み込む時にユーザーのロール、フィルター、パーミッションへのクエリーをロギングします。デフォルト値: false

sql

Rails ActiveRecord を使用した SQL クエリーをロギングします。デフォルト値: false

手順

個別のロガーを有効にするには、次の手順を実行します。

1. 任意の個別ロガーを有効化します。たとえば、**sql** と **ldap** のロガーを有効にするには、以下のコマンドを入力します。

```
# satellite-installer --foreman-loggers sql:true --foreman-loggers ldap:true
```

2. オプション: デフォルト値にロガーをリセットするには、以下のコマンドを入力します。

```
# satellite-installer --reset-foreman-loggers
```

12.3. ジャーナルへのロギングの設定

Satellite がジャーナルを使用したロギングを管理するように設定します。ジャーナルは、ログメッセージを **rsyslog** に転送し、**rsyslog** はログメッセージを `/var/log/messages` に記述します。この変更を加えた後は、ログメッセージが `/var/log/foreman/production.log` または `/var/log/foreman-proxy.log` には表示されません。

ジャーナルに関する詳細は、『Red Hat Enterprise Linux 7 システム管理者のガイド』の「[Journal の使用](#)」を参照してください。

手順

ジャーナルを使用した Satellite Server のロギングを設定するには、次の手順を実行します。

1. 以下の **satellite-installer** コマンドを入力して、ロギングを **journald** に設定します。

```
# satellite-installer --foreman-logging-level info \
--foreman-logging-type journald \
--foreman-logging-layout pattern --foreman-proxy-log JOURNAL
```

2. Apache デーモンを再起動します。

```
# satellite-maintain service restart --only httpd
```

12.4. SATELLITE が提供するログファイルディレクトリー

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12.1 レポートおよびトラブルシューティングのログファイルディレクトリー

ログファイルディレクトリー	ログファイルの内容の説明
<code>/var/log/candlepin</code>	サブスクリプションの管理
<code>/var/log/foreman</code>	Foreman
<code>/var/log/foreman-proxy</code>	Foreman プロキシ
<code>/var/log/httpd</code>	Apache HTTP サーバー

ログファイルディレクトリー	ログファイルの内容の説明
<code>/var/log/foreman-installer/satellite</code>	Satellite インストーラー
<code>/var/log/foreman-installer/capsule</code>	Capsule Server インストーラー
<code>/var/log/libvirt</code>	仮想化 API
<code>/var/log/mongodb</code>	Satellite データベース
<code>/var/log/production</code>	Foreman
<code>/var/log/pulp</code>	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 <code>/var/log/messages</code> に記録されます。
<code>/var/log/puppet</code>	設定管理
<code>/var/log/rhsm</code>	サブスクリプションの管理
<code>/var/log/tomcat6</code> および <code>/var/log/tomcat</code>	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
<code>/var/log/messages</code>	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。

12.5. ログ情報の収集ユーティリティー

ログファイルから情報を収集するユーティリティーは、2つあります。

表12.2 ログ収集ユーティリティー

コマンド	説明
------	----

コマンド	説明
foreman-debug	<p>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。</p> <p>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。</p> <p>詳細情報については、foreman-debug --help を実行してください。</p> <p>このコマンドの実行時にはタイムアウトがありません。</p>
sosreport	<p>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。</p> <p>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、「What is a sosreport and how can I create one?」を参照してください。</p> <p>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。</p>



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。

第13章 外部認証の設定

外部認証を使用して、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。外部認証を使用する場合には、このような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。

重要なユーザーおよびグループアカウント情報

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'
```

外部認証の設定シナリオ

Red Hat Satellite では、外部認証の設定において以下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。Satellite では、Satellite Web UI を介して LDAP 全体を管理できます。詳細は、「[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。IdM を使用した設定は、Satellite Web UI のみを使用して完了できず、CLI との対話が必要です。詳細は、「[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、「[フォレスト間の信頼関係のある Active Directory](#)」を参照してください。

Satellite でプロビジョニングしたホストは、Satellite Server にアクセスできるだけでなく、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、「[プロビジョニングされたホストの外部認証](#)」を参照してください。

表13.1 認証の概要

Type	認証	ユーザーグループ
IdM	Kerberos または LDAP	あり
Active Directory	Kerberos または LDAP	あり

Type	認証	ユーザーグループ
POSIX	LDAP	あり

13.1. LDAP の使用

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、まず、接続先の LDAP サーバーで使用する証明書を取得して、以下の説明のように Satellite Server のベースオペレーティングシステムでこの証明書を信頼済みとしてマークします。LDAP サーバーで中間認証局との証明書チェーンを使用する場合は、すべての証明書が取得されるように、チェーン内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、「[Red Hat Satellite で LDAP を使用するように設定する手順](#)」に進みます。

SSSD 設定の使用

このセクションでは、LDAP の直接統合について説明しますが、Red Hat では、SSSD を使用して IdM、AD、または LDAP サーバーに設定することを推奨します。SSSD により、認証プロセスの一貫性が向上されます。推奨設定の詳細は、「[Active Directory の使用](#)」を参照してください。SSSD 資格情報をキャッシュして LDAP 認証に使用することもできます。SSSD の詳細については、『[Red Hat Enterprise Linux 7 システムレベルの認証ガイド](#)』の「[SSSD の設定](#)」を参照してください。

13.1.1. セキュア LDAP 向けの TLS の設定

Satellite CLI を使用して、セキュア LDAP (LDAPS) 向けに TLS を設定します。

手順

- LDAP サーバーから証明書を取得します。
 - 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 サーバー証明書は、Satellite Server がインストールされている Red Hat Enterprise Linux システムの一時的な場所にダウンロードし、終了時に削除します。たとえば、`/tmp/example.crt` です。ファイル名の拡張子を `.cer` と `.crt` にすることが唯一の規則であり、この拡張子は、DER バイナリーまたは PEM ASCII の形式の証明書を参照できます。

- LDAP サーバーからの証明書を信頼します。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の証明書を `/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
```

- c. **httpd** サービスを再起動します。

```
# systemctl restart httpd
```

13.1.2. Red Hat Satellite で LDAP を使用するように設定する手順

Satellite Web UI で、LDAP を使用するように Satellite を設定します。

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、「[Identity Management の使用](#)」または「[Active Directory の使用](#)」を参照してください。

手順

1. Network Information System (NIS) サービスのブール値を true に設定して SELinux により LDAP の送信接続がブロックされないようにします。

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

2. **管理** > **LDAP 認証** に移動します。
3. **認証ソースの作成** をクリックします。
4. **LDAP サーバ** タブで LDAP サーバーの名前、ホスト名、ポート、およびサーバ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が。
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](#)」を参照してください。
6. **属性マッピング** タブで LDAP 属性を Satellite 属性にマッピングします。ログイン名、名、姓、メールアドレス、および写真の属性をマッピングできます。例については、「[LDAP 接続の設定例](#)」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。
10. LDAP ユーザーの新しいアカウントを設定します。
 - **Onthefly Register** チェックボックス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ます。
 - **Onthefly Register** チェックボックスを選択した場合は、LDAP ユーザーは LDAP アカウ

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 管理者が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方法は、「[ユーザーへのロールの割り当て](#)」を参照してください。

13.1.3. LDAP 設定の説明

以下の表は、Account タブの各設定の説明を示しています。

表13.2 アカウントタブの設定

設定	説明
アカウント	<p>LDAP サーバーへの読み取りアクセス権のある LDAP アカウントのユーザー名。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。</p> <pre>uid=\$login,cn=users,cn=accounts,dc=example,dc=com</pre> <p>\$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。</p> <p>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。</p>
アカウントパスワード	<p>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。</p>
ベース DN	<p>LDAP ディレクトリーの最上位のドメイン名。</p>
グローバルベース DN	<p>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。</p>
LDAP フィルター	<p>LDAP クエリーを制限するフィルター。</p>
Onthefly Register	<p>このチェックボックスを選択した場合には、LDAP ユーザーが Satellite に最初にログインしたときに、Satellite によりユーザーアカウントが作成されます。初回のログイン後に、Satellite 管理者が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。</p>
ユーザーグループの同期	<p>このオプションが選択された場合は、ユーザーのログイン時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ていない場合は、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。</p>

13.1.4. LDAP 接続の設定例

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13.3 Active Directory、Free IPA または Red Hat Identity Management、POSIX LDAP 接続 の設定例

設定	Active Directory	FreeIPA または Red Hat Identity Management	POSIX (OpenLDAP)
アカウント	DOMAIN\redhat	uid=redhat,cn=users, cn=accounts,dc=example, dc=com	uid=redhat,ou=users, dc=example,dc=com
アカウント パスワード	P@ssword	-	-
ベース DN	DC=example,DC=COM	dc=example,dc=com	dc=example,dc=com
グループ ベース DN	CN=Users,DC=example,DC= com	cn=groups,cn=accounts, dc=example,dc=com	cn=employee,ou=userclass, dc=example,dc=com
ログイン名 属性	userPrincipalName	uid	uid
名属性	givenName	givenName	givenName
姓属性	sn	sn	sn
メールアドレス 属性	mail	mail	mail



注記

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

13.1.5. 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13.4 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)

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

13.2. IDENTITY MANAGEMENT の使用

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。



注記

Identity Management は、外部認証ソースとして、シングルサインオンサポートなしでアタッチできます。詳細については、「[LDAP の使用](#)」を参照してください。

前提条件

- Satellite Server で Red Hat Enterprise Linux 7.1 または Red Hat Enterprise Linux 6.6 以降が実行されていること。
- Satellite Server のベースオペレーティングシステムが、組織の IdM 管理者によって IdM ドメインに登録されていること。

この章の例では、IdM と Satellite の設定が分離されていることを前提としています。ただし、両方のサーバーの管理者権限がある場合は、『Red Hat Enterprise Linux 7 Linux ドメイン ID、認証、およびポリシーガイド』の説明に従って IdM を設定できます。

13.2.1. Satellite Server での IdM 認証の設定

Satellite CLI で、最初に IdM サーバーにホストエントリーを作成して、IdM 認証を設定します。

手順

1. IdM サーバーで、次のコマンドを入力し、プロンプトが表示されたら、パスワードを入力して、認証します。

```
# kinit admin
```

2. 認証されたことを確認するには、次のコマンドを入力します。

```
# klist
```

3. 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の詳細は、『Red Hat Enterprise Linux 7 Linux ドメイン ID、認証、およびポリシーガイド』の「[ホストエントリー設定のプロパティ](#)」を参照してください。

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

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

サービス管理の詳細については、『Red Hat Enterprise Linux 7 Linux ドメイン ID、認証、およびポリシーガイド』の「[サービスの管理](#)」を参照してください。

5. Satellite Server で、IPA クライアントをインストールします。



警告

このコマンドは、パッケージのインストール中に Satellite サービスを再起動する可能性があります。Satellite でのパッケージのインストールと更新に関する詳細は、「[Satellite Server のベースオペレーティングシステムでのパッケージの管理](#)」を参照してください。

```
# satellite-maintain packages install ipa-client
```

- Satellite Server で、以下のコマンドを root として入力し、IdM 登録を設定します。

```
# 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。

- Satellite Server が Red Hat Enterprise Linux 7 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 **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** リポジトリに含まれます。

- 以下のコマンドを使用して、**foreman-ipa-authentication** を true に設定します。

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

- satellite-maintain** サービスを再起動します。

```
# satellite-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。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、設定済みの Kerberos シングルサインオンを活用してクライアントマシンでチケットを取得し、自動的にログインするかを選択できます。また、ワンタイムパスワードを使用した二要素認証 (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 で実行されている場合には、このユーザーは OTP を使用して Satellite に対して認証することもできます。

13.2.2. ホストベースの認証制御の設定

HBAC ルールでは、IdM ユーザーがドメイン内のどのマシンにアクセスできるかを定義します。一部のユーザーが Satellite Server にアクセスできないように、IdM サーバーで HBAC を設定できます。この方法では、ログインが許可されていないユーザーのデータベースエントリを、Satellite で作成できないようにします。HBAC の詳細については、『[Red Hat Enterprise Linux 7 Linux ドメイン ID、認証、およびポリシーガイド](#)』の「[ホストベースのアクセス制御の設定](#)」を参照してください。

IdM サーバーで、ホストベースの認証制御 (HBAC) を設定します。

手順

- IdM サーバーで、次のコマンドを入力し、プロンプトが表示されたら、パスワードを入力して、認証します。

```
# kinit admin
```

- 認証されたことを確認するには、次のコマンドを入力します。

```
# klist
```

3. 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
```

4. **satellite-prod** サービスへのアクセス権があるユーザーと 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。

5. 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
```

6. IdM サーバーで **allow_all** ルール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のルール無効にする方法については、Red Hat カスタマーポータルの記事「[How to configure HBAC rules in IdM](#)」を参照してください。

7. 「[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
```

13.3. ACTIVE DIRECTORY の使用

このセクションでは、Satellite Server 用の外部認証ソースとして直接 Active Directory (AD) を使用する方法を示します。



注記

シングルサインオンサポートなしで、Active Directory を外部認証ソースとして接続できません。詳細は、「[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。

直接 AD 統合では、ID が保存されている AD ドメインに Satellite Server が直接参加します。推奨の設定には、以下の 2 つの手順が含まれます。

- 「[Satellite Server の AD サーバーへの登録](#)」の説明に従って、Active Directory サーバーに Satellite Server を登録します。
- 「[GSS-proxy を使用した直接 AD 統合の設定](#)」の説明に従って、GSS-proxy との直接 Active Directory 統合を設定します。

13.3.1. GSS-Proxy

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。

13.3.2. Satellite Server の AD サーバーへの登録

Satellite CLI で、Active Directory サーバーに Satellite Server を登録します。

前提条件

- GSS-proxy と nfs-utils がインストールされていること。
GSS-proxy と nfs-utils をインストールします。

```
# satellite-maintain packages install gssproxy nfs-utils
```

手順

1. 必要なパッケージをインストールします。

```
# satellite-maintain packages install sssd adcli realmd ipa-python-compat krb5-workstation samba-common-tools
```

2. Satellite Server を AD サーバーに登録します。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
```

13.3.3. GSS-proxy を使用した直接 AD 統合の設定

Satellite CLI で、GSS-proxy を使用する直接 Active Directory 統合を設定します。

前提条件

- Satellite が、Active Directory サーバーに登録されていること。
詳細は、「[Satellite Server の AD サーバーへの登録](#)」を参照してください。

手順

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. Apache ユーザーの有効なユーザー ID を特定します。

```
# id apache
```

Apache ユーザーには keytab ファイルへのアクセス権を割り当てないでください。

5. 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 = ID_of_Apache_User
```

6. 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/
```

7. 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
```

8. Satellite の IPA 認証を有効にします。

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

9. **gssproxy** サービスを起動して、有効にします。

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

10. 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
```

11. **httpd** サービスを起動して、有効にします。

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

12. SSO が想定どおりに動作していることを確認します。

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。

- a. 次のコマンドを使用して、LDAP ユーザーの Kerberos チケットを取得します。

```
# kinit ldapuser
```

- b. 以下のコマンドを使用して、Kerberos チケットを表示します。

```
# klist
```

- c. 以下のコマンドを使用して、SSO 認証に成功時の出力を表示します。

```
# 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>
```

13.3.4. Web ブラウザーでの Kerberos の設定

Firefox ブラウザーの設定の詳細は、『Red Hat Enterprise Linux 7 システムレベルの認証ガイド』の「[Firefox でシングルサインオンに Kerberos を使用する設定](#)」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、Satellite Server をローカルイントラネットまたは信頼済みサイトのリストに追加し、**統合 Windows 認証を使用する** の設定にチェックを入れます。詳細については、Internet Explorer のマニュアル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
```

ここでは、`foreman` は PAM サービスの名前です。GPO の詳細については、『[Red Hat Enterprise Linux 7 Windows 統合ガイド](#)』の「[グループポリシーオブジェクトのアクセス制御](#)」を参照してください。

13.3.5. フォレスト間の信頼関係のある Active Directory

Kerberos では、**cross-forest trust** を作成して、2つの異なるドメインフォレスト間の関係を定義できます。ドメインフォレストとは、ドメインの階層構造のことで、AD と IdM の両方でフォレストが形成されます。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は、『[Red Hat Enterprise Linux 7 Windows 統合ガイド](#)』の「[Active Directory および Identity Management によるフォレスト間の信頼作成](#)」を参照してください。

Satellite 側から見ると、設定プロセスは、フォレスト間の信頼を設定せずに IdM サーバーと統合する場合と同じです。Satellite Server は IPM ドメインに登録し、「[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。

13.3.6. フォレスト間信頼を使用する IdM サーバーの設定

IdM サーバーで、**cross-forest trust** を使用するようにサーバーを設定します。

手順

1. HBAC を有効にします。
 - a. 外部グループを作成して、この外部グループに AD グループを追加します。
 - b. 新しい外部グループを POSIX グループに追加します。
 - c. HBAC ルールで POSIX グループを使用します。
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。
 - この AD ユーザー属性を `/etc/sssds/sssds.conf` の `nss` セクションと `domain` セクションに追加します。
例を示します。

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

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

13.4. 外部ユーザーグループの設定

Satellite は、自動的に、外部ユーザーグループに外部ユーザーを関連付けることはありません。Satellite 上の外部ソースと同じ名前のユーザーグループを作成する必要があります。こうすることで、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が付与されます。

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。

外部ユーザーに追加の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、このユーザーを追加します。次に、このグループに必要なロールを割り当てます。

前提条件

- LDAP サーバーを使用する場合は、Satellite が LDAP 認証を使用するように設定する。詳細は、「[LDAP の使用](#)」を参照してください。
LDAP ソースから外部ユーザーグループを使用する場合は、アカウントユーザー名の代わりにとして `$login` 変数を使用できず、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。
- IdM または AD サーバーを使用する場合は、Satellite が IdM または AD 認証を使用するように設定する。詳細は、[13章 外部認証の設定](#)を参照してください。
- 少なくとも1人の外部ユーザーが初回認証されることを確認する。
- 使用する外部グループ名をメモする。外部ユーザーのグループメンバーシップを確認するには、以下のコマンドを入力します。

```
# id username
```

外部ユーザーグループの設定:

1. Satellite Web UI で、**管理 > ユーザーグループ** に移動して、**ユーザーグループの作成** をクリックします。
2. 新規ユーザーグループの名前を指定します。外部ユーザーグループのリフレッシュ時にユーザーが自動的に追加されるのを避けるため、ユーザーを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** の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。

13.5. LDAP の外部ユーザーグループのリフレッシュ

ユーザーのログイン時にユーザーのグループメンバーシップを自動的に同期するように LDAP ソースを設定するには、**認証ソース** ページで、**ユーザーグループの同期** オプションを選択します。このオプションが選択されていない場合、デフォルトで、LDAP ユーザーグループは、30 分ごとに LDAP 認証ソースを同期するようにスケジュールされた cron ジョブで自動的にリフレッシュされます。

LDAP 認証ソースのユーザーグループが、次のスケジュールタスクが実行されるまでの間に変更された場合に、ユーザーが不正な外部ユーザーグループに割り当てられることがあります。これはスケジュールされたタスクの実行時に、自動的に修正されます。

以下の手順を使用して、LDAP ソースを手動でリフレッシュします。

手順

1. **管理** > **ユーザーグループ** に移動し、ユーザーグループを選択します。
2. **外部グループ** タブに移動し、必要なユーザーグループの右側にある **リフレッシュ** をクリックします。

CLI をご利用の場合

以下のコマンドを実行します。

```
# foreman-rake ldap:refresh_usergroups
```

13.6. IDM または AD の外部ユーザーグループのリフレッシュ

IdM または AD ベースの外部ユーザーグループは、グループメンバーが Satellite にログインしたときのみリフレッシュされます。Satellite Web UI 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ず、このような変更がされた場合には、次のグループリフレッシュ時に上書きされます。

13.7. プロビジョンされたホストの外部認証

以下のセクションを使用して、IdM レルムがサポートされるように Satellite Server または Capsule Server を設定し、IdM レルムグループにホストを追加します。

前提条件

プロビジョニングされたホストの外部認証を設定するには、以下の設定が必要です。

- Satellite Server をコンテンツ配信ネットワークに登録しておくか、外部の Capsule Server を Satellite Server に登録しておく。
- Red Hat Identity Management などのレルムまたはドメインプロバイダーがデプロイされている。

Red Hat Satellite Server または Red Hat Satellite Capsule Server に IdM パッケージをインストールして設定する手順:

プロビジョニングされたホストに IdM を使用するには、以下の手順を実行して、Red Hat Satellite Server または Red Hat Satellite Capsule Server に IdM パッケージをインストールして設定します。

1. Satellite Server または Capsule Server に **ipa-client** パッケージをインストールします。

- Satellite Server で以下のコマンドを入力します。

```
# satellite-maintain packages install ipa-client
```

- Capsule Server で以下のコマンドを入力します。

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

2. サーバーを IdM クライアントとして設定します。

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

3. Red Hat Identity Management でレルムプロキシユーザー **realm-capsule** と、関連のロールを作成します。

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

以下の手順で必要となるので、返されたプリンシパル名と、アイデンティティ管理サーバーの設定情報をメモします。

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

使用する Satellite および全 Capsule で次の手順を実行します。

1. 同じプリンシパルおよびレルムに追加する Capsule Server に、**/root/freeipa.keytab** ファイルをコピーします。

```
# scp /root/freeipa.keytab root@capsule.example.com:/etc/foreman-proxy/freeipa.keytab
```

2. **/root/freeipa.keytab** ファイルを **/etc/foreman-proxy** ディレクトリーに移動して、所有者を **foreman-proxy** ユーザーに設定します。

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

3. レルムに追加する全 Capsule で、**t**以下のコマンドを入力します。Satellite に統合された Capsule を使用する場合には、Satellite Server でこのコマンドを入力します。

```
# 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
```

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使用できます。

4. **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
```

5. オプション: 既存の Satellite Server または Capsule Server で IdM を設定する場合には、以下の手順を実行して、設定の変更が適用されていることを確認します。

- a. **foreman-proxy** サービスを再起動します。

```
# systemctl restart foreman-proxy
```

- b. 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。
- c. IdM 用に設定した Capsule の場所を特定して、アクション コラムのリストから **リフレッシュ** を選択します。

IdM 対応の Capsule のレルムを作成する手順

統合型または外部の Capsule に IdM を設定した後に、レルムを作成して、IdM が設定された Capsule にレルムを追加する必要があります。

レルムを作成するには、以下の手順を行います。

1. Satellite Web UI で、インフラストラクチャー > レルム に移動して、**レルムの作成** をクリックします。
2. **名前** フィールドには、レルムの名前を入力します。
3. **レルムのタイプ** 一覧から、レルムのタイプを選択します。
4. **レルム Capsule** 一覧から、IdM を設定した Capsule Server を選択します。
5. **ロケーション** タブをクリックして、**ロケーション** 一覧から、新しいレルムを追加するロケーションを選択します。
6. **組織** タブをクリックして、**組織** 一覧から、新規レルムを追加する組織を選択します。
7. **送信** をクリックします。

レルム情報でのホストグループの更新

使用するホストグループを、新しいレルム情報で更新する必要があります。

1. **設定** > **ホストグループ** に移動して、更新するホストグループを選択し、**ネットワーク** タブをクリックします。
2. **レルム** 一覧から、この手順の一部で作成したレルムを選択して **送信** をクリックします。

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。

Satellite Server または Capsule Server は更新を 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 --desc=hostgroup_description
```

2. automembership ルールを作成します。

```
# ipa automember-add --type=hostgroup hostgroup_name automember_rule
```

以下のオプションを使用できる場所:

- **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 ルールの識別に使用する名前を追加します。

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
-----
```

以下のオプションを使用できる場所:

- **automember-add-condition** では、グループメンバーを識別する正規表現の条件を追加します。
- **--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、正規表現パターンで一致する値を識別します。
- **hostgroup_name**: ターゲットホストグループの名前を識別します。

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。

第14章 リソースの監視

本章では、管理システムの監視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、**監視 > 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またはエラーを検出するためにこのセクションを監視します。

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サマリーです。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、これらのホストを監視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 アクション

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、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 時間ごとにリフレッシュされ、新規イベントが利用可能となると通知エリアがリフレッシュされます。

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 の監視

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、コンピュータリソース、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 の監視

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

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)** 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** コラム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、また 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 Server 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 **リフレッシュ** 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. サービスの監視

インフラストラクチャー > **Capsules (スマートプロキシ)** 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)** 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 イベントのサマリー、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. トレンドの監視

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ン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. **監視** > **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. **監視** > **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、または入力を続け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) を受け入れません。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 <code>_</code> 、ゼロを含む任意の数の文字の場合の <code>%</code> または <code>*</code> 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ず (例: <code>%rhel7%</code>)。	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。
<	LESS THAN		registered_at <= Yesterday 検索結果では、昨日以前に登録されたホストが返されます。
^	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、検索結果は 1 つ以上のホストグループに割り当てられたクラスを返します。
NOT HAS or null?			not has hostgroup または null? hostgroup ホストの概要を表示するダッシュボードで、検索結果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。

記述された構文に従う単純なクエリを組み合わせ、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、空白文字は 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とも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 **active** または **disabled** 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

このセクションには、**Administer > Settings** に移動して、Satellite Web UI で編集できる設定に関する重要な情報または既知の問題が含まれています。

表A.1 一般的な設定情報

設定	説明
DB キャッシュの修正	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。

表A.2 プロビジョニングの設定情報

設定	説明
名前ジェネレーターのタイプ	<p>新規ホスト作成時のホスト名の生成方法を指定します。</p> <p>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、命名方法がわからないユーザーには便利です。</p> <p>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する場合に便利です。</p> <p>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。</p>
Safemode レンダリング	<p>プロビジョニングテンプレートのセーフモードレンダリングを有効にします。デフォルトの推奨オプション Yes は、Satellite 内でホワイトリストに記載されていない変数およびオブジェクトへのアクセスを拒否します。</p> <p>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 で完全なり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。</p>

設定	説明
Satellite に保存されているファクトの除外パターン	BZ#1759111 が解決されるまで、 docker* などのワイルドカード値を使用して docker で始まるすべてのファクトを除外する場合は、除外する用語が名前の一部に含まれるファクトも除外されることに注意してください。
一致する識別子を持つインターフェースを無視	BZ#1759111 が解決されるまで、 docker* などのワイルドカード値を使用して docker で始まるすべてのファクトを無視する場合は、無視する用語が名前的一部分に含まれるファクトも除外されることに注意してください。