Red Hat Satellite 6.4

Administering Red Hat Satellite

A guide to administering Red Hat Satellite.

Last Updated: 2019-12-03

Red Hat Satellite 6.4 Administering Red Hat Satellite

A guide to administering Red Hat Satellite.

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

Legal Notice

Copyright © 2019 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.

Abstract

This guide provides instructions on how to configure and administer a Red Hat Satellite 6 Server. Before continuing with this workflow you must have successfully installed a Red Hat Satellite 6 Server and any required Capsule Servers.

Table of Contents

CHAPTER 1. ACCESSING RED HAT SATELLITE

After Red Hat Satellite has been installed and configured, use the web user interface to log in to Satellite for further configuration.

1.1. INSTALLING THE KATELLO ROOT CA CERTIFICATE

The first time you log on to Satellite, you might see a warning informing you that you are using the default self-signed certificate and you might not be able to connect this browser to Satellite until the root CA certificate is installed in the browser. Use the following procedure to locate the root CA certificate on Satellite and to install it in your browser.

Prerequisites

Your Red Hat Satellite is installed and configured.

Procedure

1. Identify the fully qualified domain name of your Satellite Server:

   ```
   # hostname -f
   ```

2. Access the **pub** directory on your Satellite Server using a web browser pointed to the fully qualified domain name:

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

3. When you access Satellite for the first time, an untrusted connection warning displays in your web browser. Accept the self-signed certificate and add the Satellite URL as a security exception to override the settings. This procedure might differ depending on the browser being used. Ensure that the Satellite URL is valid before you accept the security exception.

4. Select **katello-server-ca.crt**.

5. Import the certificate into your browser as a certificate authority and trust it to identify websites.

Importing the Katello Root CA Certificate Manually

If you cannot add a security exception in your browser, import the Katello root CA certificate manually.

1. From the Satellite CLI, copy the **katello-server-ca.crt** file to the machine you use to access the web UI:

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

2. In the browser, import the **katello-server-ca.crt** certificate as a certificate authority and trust it to identify websites.

1.2. LOGGING ON TO SATELLITE

Use the web user interface to log on to Satellite for further configuration.

Prerequisites

Ensure that the Katello root CA certificate is installed in your browser. For more information, see Section 1.1, "Installing the Katello Root CA Certificate" .

Procedure

1. Access the Satellite Server using a web browser pointed to the fully qualified domain name:

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

2. Enter the user name and password created during the configuration process. If a user was not created during the configuration process, the default user name is *admin*. If you have problems logging on, you can reset the password. For more information, see Section 1.5, "Resetting the Administrative User Password".

1.3. NAVIGATION TABS IN THE SATELLITE WEB UI

Use the navigation tabs to browse the Satellite web UI.

Table 1.1. Navigation Tabs

Navigation Tabs	Description
Any Context	Clicking this tab changes the organization and location. If no organization or location is selected, the default organization is *Any Organization* and the default location is *Any Location*. Use this tab to change to different values.
Monitor	Provides summary dashboards and reports.
Content	Provides content management tools. This includes Content Views, Activation Keys, and Life Cycle Environments.
Containers	Provides container management tools.
Hosts	Provides host inventory and provisioning configuration tools.
Configure	Provides general configuration tools and data including Host Groups and Puppet data.
Infrastructure	Provides tools on configuring how Satellite 6 interacts with the environment.
Red Hat Insights	Provides Red Hat Insights management tools.
Red Hat Access	Provides access to Red Hat knowledgebase, Satellite log files, and support cases.
User Name	Provides user administration where users can edit their personal information.

Navigation Tabs	Description
🔔	Provides event notifications to keep administrators informed of important environment changes.
Administer	Provides advanced configuration for settings such as Users and RBAC, as well as general settings.

1.4. CHANGING THE PASSWORD

These steps show how to change your password.

To Change your Red Hat Satellite Password:

1. Click your user name at the top right corner.
2. Select **My Account** from the menu.
3. In the **Current Password** field, enter the current password.
4. In the **Password** field, enter a new password.
5. In the **Verify** field, enter the new password again.
6. Click the **Submit** button to save your new password.

1.5. RESETTING THE ADMINISTRATIVE USER PASSWORD

Use the following procedures to reset the administrative password to randomly generated characters or to set a new administrative password.

To Reset the Administrative User Password:

To reset the password to randomly generated characters, complete the following procedure:

1. Log on to the base operating system where Satellite Server is installed.
2. Enter the following command to reset the password:

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

3. Use this password to reset the password in the Satellite web UI.
4. Edit the **~/.hammer/cli.modules.d/foreman.yml** file on Satellite Server to add the new password:

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

Unless you update the **~/.hammer/cli.modules.d/foreman.yml** file, you cannot use the new password with Hammer CLI.

To Set a New Administrative User Password:

To change the administrative user password to a new password, complete the following steps:

1. Log on to the base operating system where Satellite Server is installed.
2. To set the password, enter the following command:

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

3. Edit the **~/.hammer/cli.modules.d/foreman.yml** file on Satellite Server to add the new password:

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

Unless you update the **~/.hammer/cli.modules.d/foreman.yml** file, you cannot use the new password with Hammer CLI.

1.6. SETTING A CUSTOM MESSAGE ON THE LOGIN PAGE

To Set a Custom Message on the Login Page:

1. Navigate to **Administer** > **Settings**, and click the **General** tab.
2. Click the edit button next to **Login page footer text**, and enter the desired text to be displayed on the login page. For example, this text may be a warning message required by your company.
3. Click **Save**.
4. Log out of the Satellite’s web UI and verify that the custom text is now displayed on the login page below the Satellite version number.

CHAPTER 2. STARTING AND STOPPING RED HAT SATELLITE

Satellite provides the **foreman-maintain service** command to manage Satellite services from the command line. This is useful when creating a backup of Satellite. For more information on creating backups, see Section 8.1, "Backing up Satellite Server or Capsule Server" .

After installing Satellite with the **satellite-installer** command, all Satellite services are started and enabled automatically. View the list of these services by executing:

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

To see the status of running services, execute:

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

To stop all Satellite services, execute:

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

To start all Satellite services, execute:

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

To restart all Satellite services, execute:

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

CHAPTER 3. MIGRATING TO EXTERNAL DATABASES

As part of the installation process for Red Hat Satellite, the **satellite-installer** command installs MongoDB and PostgreSQL databases on the same server as Satellite. In certain Satellite deployments, using external databases can help with the server load. If your Satellite deployment requires external databases, you can migrate your internal databases to external databases.

Depending on your requirements, you can use external databases for either MongoDB or PostgreSQL database, or both.

Red Hat does not provide support or tools for external database maintenance. This includes backups, upgrades, and database tuning. Customers using an external database require their own database administrator to support and maintain the database.

To view whether your Satellite Server has embedded or external databases, you can query the status of your databases. For example, enter the following command with the **--only** and add **postgresql** or **rh-mongodb34-mongod**:

For PostgreSQL, enter the following command:

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

For MongoDB, enter the following command:

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

If your Satellite deployment requires external databases, use the following information to set up and point to external databases from Satellite.

3.1. MONGODB AS AN EXTERNAL DATABASE CONSIDERATIONS

Pulp uses the MongoDB database. If you want to use MongoDB as an external database, the following information can help you discern if this option is right for your Satellite configuration.

Advantages of External MongoDB

- Increase in free memory and free CPU on Satellite
- Flexibility to tune the MongoDB server's system without adversely affecting Satellite operations

Disadvantages of External MongoDB

- Increase in deployment complexity that can make troubleshooting more difficult
- An external MongoDB server is an additional system to patch and maintain
- If either the Satellite or the Mongo database server suffers a hardware or storage failure, Satellite is not operational
- If there is latency between the Satellite and the external database server, performance can suffer

If you suspect that your Mongo database is slow, you can work with Red Hat Support to troubleshoot. You might be encountering a configuration problem or existing performance problems with Satellite 6 that moving to an external database server might not help. Red Hat Support can examine existing known issues and also work with the Satellite Engineering team to determine the root cause.

3.2. POSTGRESQL AS AN EXTERNAL DATABASE CONSIDERATIONS

Foreman, Katello, and Candlepin use the PostgreSQL database. If you want to use PostgreSQL as an external database, the following information can help you discern if this option is right for your Satellite configuration.

Advantages of External PostgreSQL:

- Increase in free memory and free CPU on Satellite
- Flexibility to set **shared_buffers** on the PostgreSQL database to a high number without the risk of interfering with other services on Satellite
- Flexibility to tune the PostgreSQL server's system without adversely affecting Satellite operations

Disadvantages of External PostgreSQL

- Increase in deployment complexity that can make troubleshooting more difficult
- The external PostgreSQL server is an additional system to patch and maintain
- If either Satellite or the PostgreSQL database server suffers a hardware or storage failure, Satellite is not operational
- If there is latency between the Satellite server and database server, performance can suffer

If you suspect that the PostgreSQL database on your Satellite is causing performance problems, use the information in Satellite 6: How to enable postgres query logging to detect slow running queries to determine if you have slow queries. Queries that take longer than one second are typically caused by performance issues with large installations, and moving to an external database might not help. If you have slow queries, contact Red Hat Support.

3.3. OVERVIEW

To create and use external databases for Satellite, you must complete the following procedures:

1. Use Storage Requirements and Guidelines in *Installing Satellite Server from a Connected Network* to plan the storage requirements for your external databases.
2. Prepare PostgreSQL with databases for Foreman and Candlepin and respective Foreman and Candlepin users with ownership roles.
3. Prepare MongoDB with the Pulp user owning the **pulp_database**.
4. Back up your existing Satellite databases.
5. Migrate the internal Satellite databases to external databases.
6. Edit the arguments of the **satellite-installer** command to point to the new databases, and run **satellite-installer**.

Preparing Red Hat Enterprise Linux Server 7 for Database Installation

You require a freshly provisioned system with the latest Red Hat Enterprise Linux Server 7 that meets the storage requirements from Storage Requirements and Guidelines in the *Installing Satellite Server from a Connected Network*.

Subscriptions for Red Hat Software Collections and Red Hat Enterprise Linux do not provide the correct service level agreement for using Satellite with external databases. You must also attach a Satellite subscription to the base system that you want to use for the external database.

1. Attach a Satellite subscription to your server. For more information, see Identifying and Attaching the Satellite Subscription to the Host in the *Installing Satellite Server from a Connected Network*.

2. To install MongoDB and PostgreSQL servers on Red Hat Enterprise Linux Server 7, you must disable all repositories and enable only the following repositories:

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

3.4. INSTALLING MONGODB

You can install only the same version of MongoDB that is installed with the **satellite-installer** tool during an internal database installation. You can install MongoDB using Red Hat Software Collections (RHSCL) repositories or from an external source, as long as the version is supported. Satellite supports MongoDB version 3.4.

1. To install MongoDB, enter the following command:

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

2. Start and enable the **rh-mongodb34-mongod** service:

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

3. Create a Pulp user on MongoDB:

   ```
   # mongo pulp_database \
   --eval "db.createUser({user:'pulp',pwd:'pulp_password',roles:[{role:'dbOwner',
   db:'pulp_database'},{ role: 'readWrite', db: 'pulp_database'}]})"
   ```

4. Edit the **/etc/opt/rh/rh-mongodb34/mongod.conf** file to enable authentication in the **security** section:

   ```
   security:
     authorization: enabled
   ```

5. In the **/etc/opt/rh/rh-mongodb34/mongod.conf** file, specify the bind IP:

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

6. Restart the **rh-mongodb34-mongod** service:

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

7. Open port 27017 for MongoDB:

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

8. From Satellite Server, test that you can access the database. If the connection succeeds, the command returns **1**.

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

3.5. INSTALLING POSTGRESQL

You can install only the same version of PostgreSQL that is installed with the **satellite-installer** tool during an internal database installation. Satellite supports only a specific version of PostgreSQL that is available through Red Hat Enterprise Linux Server 7 repositories. You can install PostgreSQL using Red Hat Enterprise Linux Server 7 repositories or from an external source, as long as the version is supported. For more information about the repository that contains the supported version of PostgreSQL, and what version is supported, see the Package Manifest.

1. To install PostgreSQL, enter the following command:

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

+. To initialize, start, and enable PostgreSQL, enter the following commands:

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

2. Edit the **/var/lib/pgsql/data/postgresql.conf** file:

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

3. Remove the **#** and edit the following line to listen for inbound connections:

```
listen_addresses = '*'
```

4. Edit the **/var/lib/pgsql/data/pg_hba.conf** file:

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

5. Add the following line to the file:

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

6. Restart **postgreSQL** service to update with the changes:

```
# systemctl restart postgresql
```

7. Switch to the **postgres** user and start the PostgreSQL client:

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

8. Create two users, databases, and dedicated roles, one for Foreman and one for Candlepin:

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

9. Open the **postgresql** port on the external PostgreSQL server:

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

10. From Satellite Server, test that you can access the database. If the connection succeeds, the commands return **1**.

```
# 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"
```

To Migrate to External Databases

To migrate internal databases to external databases, complete the following steps:

1. On Satellite Server, stop Satellite services:

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

2. Start the **postgreSQL** and **mongod** services:

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

3. Back up the internal databases:

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

4. Transfer the data to the new external databases:

```
PGPASSWORD='Satellite_Password' pg_restore -h postgres.example.com -U foreman -d
foreman < /var/migration_backup/foreman.dump
PGPASSWORD='Candlepin_Password' pg_restore -h postgres.example.com -U candlepin -
d candlepin < /var/migration_backup/candlepin.dump
mongorestore --host mongo.example.com --db pulp_database --username pulp --password
pulp_password /var/migration_backup/mongo_dump
```

5. Use the **satellite-installer** command to update Satellite to point to the new databases:

```
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
```

CHAPTER 4. MANAGING ANSIBLE ROLES

In Satellite, you can import Ansible roles and Red Hat Enterprise Linux system roles to help with automation of routine tasks. Ansible is enabled by default on Satellite and Capsule.

If you use custom or third party Ansible roles, you must add the roles to the **/etc/ansible/roles** directory of the Capsule or Satellite where you want to use them.

For more information about support levels for Ansible in Satellite, see the *Support for Ansible in Satellite* section of the New Features and Enhancements in the *Release Notes*.

You must import the Ansible roles into Satellite Server from the **/etc/ansible/roles** directory before you can use them.

4.1. IMPORTING ANSIBLE ROLES

You can import Ansible roles from a Capsule that has Ansible enabled or from the **/etc/ansible/roles** directory where Satellite Server is installed.

To import Ansible roles, complete the following steps:

1. In the Satellite web UI, navigate to **Configure** > **Roles** and click the Capsule that contains the roles that you want to import.

2. From the list of Ansible roles, select the check box of the roles you want to import, and then click **Update**.

4.2. ADDING RED HAT ENTERPRISE LINUX SYSTEM ROLES

Red Hat Enterprise Linux System Roles, which was introduced in Red Hat Enterprise Linux 7.4 as a Technology Preview, is a configuration interface for Red Hat Enterprise Linux subsystems. You can use Red Hat Enterprise Linux System Roles to add Ansible roles in Satellite. Using Ansible Roles in Satellite can make configuration faster and easier.

For more information about Red Hat Enterprise Linux System Roles, see Red Hat Enterprise Linux System Roles.

Before subscribing to the Extras channels, see the Red Hat Enterprise Linux Extras Product Life Cycle article.

To Add Red Hat Enterprise Linux System Roles:

1. Ensure that the **rhel-7-server-extras-rpms** repository is enabled.

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

2. Install the **rhel-system-roles** package.

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

   The **rhel-system-roles** package downloads to **/usr/share/ansible/roles/**. You can view and make any modifications that you want to the files before you import.

3. In the Satellite web UI, navigate to **Configure** > **Roles** and click the Capsule that contains the roles that you want to import.

4. From the list of Ansible roles, select the check box of the roles you want to import, and then click **Update**.

You can now assign Ansible roles to hosts or host groups. For more information, see Assigning Ansible Roles to Existing Hosts in the *Managing Hosts* guide.

You can also add the modules contained in these roles to your Ansible playbooks by adding them to Ansible Job Templates. You must include the **hosts:all** line in the job template. For more information, see Red Hat Enterprise Linux (RHEL) System Roles .

CHAPTER 5. MANAGING USERS AND ROLES

A User defines a set of details for individuals using the system. Users can be associated with organizations and environments, so that when they create new entities, the default settings are automatically used. Users can also have one or more *roles* attached, which grants them rights to view and manage organizations and environments. See Section 5.1, "User Management" for more information on working with users.

You can manage permissions of several users at once by organizing them into user groups. User groups themselves can be further grouped to create a hierarchy of permissions. See Section 5.2, "Creating and Managing User Groups" for more information on creating user groups.

Roles define a set of permissions and access levels. Each role contains one on more *permission filters* that specify the actions allowed for the role. Actions are grouped according to the *Resource type*. Once a role has been created, users and user groups can be associated with that role. This way, you can assign the same set of permissions to large groups of users. Red Hat Satellite provides a set of predefined roles and also enables creating custom roles and permission filters as described in Section 5.3, "Creating and Managing Roles".

5.1. USER MANAGEMENT

As an administrator, you can create, modify and remove Satellite users. You can also configure access permissions for a user or a group of users by assigning them different *roles*.

5.1.1. Creating a User

Use the Satellite web UI to create a user.

Procedure

1. Navigate to **Administer** > **Users**.
2. Click **Create User**.
3. In the **Login** field, enter a username for the user.
4. In the **Firstname** and **Lastname** fields, enter the real first name and last name of the user.
5. In the **Mail** field, enter the user's email address.
6. In the **Description** field, add a description of the new user.
7. Select a specific language for the user from the **Language** list.
8. Select a timezone for the user from the **Timezone** list.
   By default, Satellite Server uses the language and timezone settings of the user's browser.
9. Set a password for the user:
   a. From the **Authorized by** list, select the source by which the user is authenticated.
      - **INTERNAL**: to enable the user to be managed inside Satellite Server.
      - **LDAP or IdM**: to configure external authentication as described in Chapter 13, *Configuring External Authentication*.

b. Enter an initial password for the user in the **Password** field and the **Verify** field.

10. Click **Submit** to create the user.

5.1.2. Assigning Roles to a User

Assign roles to a user using the Satellite web UI.

Procedure

1. Navigate to **Administer** > **Users**.
2. Click the **username** of the user to be assigned one or more roles.

   NOTE

   If a user account is not listed, check that you are currently viewing the correct organization. To list all the users in Satellite, click **Default Organization** and then **Any Organization**.

3. Click the **Locations** tab, and select a location if none is assigned.
4. Click the **Organizations** tab, and check that an organization is assigned.
5. Click the **Roles** tab to display the list of available roles.
6. Select the roles to assign from the **Roles** list.
   To grant all the available permissions, select the **Admin** check box.
7. Click **Submit**.

To view the roles assigned to a user, click the **Roles** tab; the assigned roles are listed under **Selected items**. To remove an assigned role, click the role name in **Selected items**.

5.1.3. SSH Keys

Adding SSH keys to a user allows deployment of SSH keys during provisioning.

For information on deploying SSH keys during provisioning, see Deploying SSH Keys during Provisioning in the *Red Hat Satellite Provisioning Guide*.

For information on SSH keys and SSH key creation, see Generating Key Pairs in the *Red Hat Enterprise Linux 7 System Administrator's Guide*.

5.1.4. Managing SSH Keys for a User

Add or remove SSH keys for a user from the Satellite web UI.

NOTE

Make sure that you are logged in to the web UI as an Admin user of Red Hat Satellite or a user with the *create_ssh_key* permission enabled for adding SSH key and *destroy_ssh_key* permission for removing a key.

Procedure

1. Navigate to **Administer** > **Users**.
2. From the **Username** column, click on the username of the required user.
3. Click on the **SSH Keys** tab.
   - To Add SSH key
     i. Prepare the content of the public SSH key in a clipboard.
     ii. Click **Add SSH Key**.
     iii. In the **Key** field, paste the public SSH key content from the clipboard.
     iv. In the **Name** field, enter a name for the SSH key.
     v. Click **Submit**.
   - To Remove SSH key
     i. Click **Delete** on the row of the SSH key to be deleted.
     ii. Click **OK** in the confirmation prompt.

5.1.5. Email Notifications

Email notifications are created by Satellite Server periodically or after completion of certain events. The periodic notifications can be sent daily, weekly or monthly.

The events that trigger a notification are the following:

- Host build
- Content View promotion
- Error reported by host
- Repository sync

Users do not receive any email notifications by default. An administrator can configure users to receive notifications based on criteria such as the type of notification, and frequency.

NOTE

If you want email notifications sent to a group's email address, instead of an individual's email address, create a user account with the group's email address and minimal Satellite permissions, then subscribe the user account to the desired notification types.

IMPORTANT

Satellite Server does not enable outgoing emails by default, therefore you must review your email configuration. For more information, see Configuring Satellite Server for Outgoing Emails in *Installing Satellite Server from a Connected Network* .

5.1.6. Configuring Email Notifications

Configure email notifications for a user from the Satellite web UI.

Procedure

1. Navigate to **Administer** > **Users**.
2. Click the **Username** of the user you want to edit.
3. On the **User** tab, verify the value of the **Mail** field. Email notifications will be sent to the address in this field.
4. On the **Email Preferences** tab, select **Mail Enabled**.
5. Select the notifications you want the user to receive using the drop-down menus next to the notification types.

   > **NOTE**
   >
   > The **Audit Summary** notification can be filtered by entering the required query in the **Mail Query** text box.

6. Click **Submit**.
   The user will start receiving the notification emails.

5.1.7. Testing Email Delivery

To verify the delivery of emails, send a test email to a user. If the email gets delivered, the settings are correct.

Procedure

1. In the Satellite web UI, navigate to **Administer** > **Users**.
2. Click on the username.
3. On the **Email Preferences** tab, click **Test email**.
   A test email message is sent immediately to the user’s email address.

If the email is delivered, the verification is complete. Otherwise, you must perform the following diagnostic steps:

a. Verify the user’s email address.

b. Verify Satellite Server’s email configuration.

c. Examine firewall and mail server logs.

5.1.8. Testing Email Notifications

To verify that users are correctly subscribed to notifications, trigger the notifications manually.

Procedure

- To trigger the notifications, execute the following command:

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

  Replace *frequency* with one of the following:

  - daily
  - weekly
  - monthly

This triggers all notifications scheduled for the specified frequency for all the subscribed users. If every subscribed user receives the notifications, the verification succeeds.

NOTE

Sending manually triggered notifications to individual users is currently not supported.

5.1.9. Notification Types

The following are the notifications created by Satellite:

- **Audit summary**: A summary of all activity audited by the Satellite Server.
- **Host built**: A notification sent when a host is built.
- **Host errata advisory**: A summary of applicable and installable errata for hosts managed by the user.
- **OpenSCAP policy summary**: A summary of OpenSCAP policy reports and their results.
- **Promote errata**: A notification sent only after a Content View promotion. It contains a summary of errata applicable and installable to hosts registered to the promoted Content View. This allows a user to monitor what updates have been applied to which hosts.
- **Puppet error state**: A notification sent after a host reports an error related to Puppet.
- **Puppet summary**: A summary of Puppet reports.
- **Sync errata**: A notification sent only after synchronizing a repository. It contains a summary of new errata introduced by the synchronization.

5.2. CREATING AND MANAGING USER GROUPS

5.2.1. User Groups

With Red Hat Satellite, you can assign permissions to groups of users. You can also create user groups as collections of other user groups. If using an external authentication source, you can map Satellite user groups to external user groups as described in Section 13.4, “Configuring External User Groups” .

User groups are defined in an organizational context, meaning that you must select an organization before you can access user groups.

5.2.2. Creating a User Group

Use the Satellite web UI to create a user group.

Procedure

1. Navigate to **Administer** > **User Groups**.
2. Click **Create User group**.
3. On the **User Group** tab, specify the name of the new user group and select group members:
   - Select the previously created user groups from the **User Groups** list.
   - Select users from the **Users** list.
4. On the **Roles** tab, select the roles you want to assign to the user group. Alternatively, select the **Admin** check box to assign all available permissions.
5. Click **Submit**.

5.2.3. Removing a User Group

Use the Satellite web UI to remove a user group.

Procedure

1. Navigate to **Administer** > **User Groups**.
2. Click **Delete** to the right of the user group you want to delete.
3. In the alert box that appears, click **OK** to delete a user group.

5.3. CREATING AND MANAGING ROLES

Red Hat Satellite provides a set of predefined roles with permissions sufficient for standard tasks, as listed in Section 5.3.7, “Predefined Roles Available in Satellite” . It is also possible to configure custom roles, and assign one or more permission filters to them. Permission filters define the actions allowed for a certain resource type. Certain Satellite plug-ins create roles automatically.

5.3.1. Creating a Role

Use the Satellite web UI to create a role.

Procedure

1. Navigate to **Administer** > **Roles**.
2. Click **Create Role**.
3. Provide a **Name** for the role.
4. Click **Submit** to save your new role.

To serve its purpose, a role must contain permissions. After creating a role, proceed to Section 5.3.3, "Adding Permissions to a Role".

5.3.2. Cloning a Role

Use the Satellite web UI to clone a role.

Procedure

1. Navigate to **Administer** > **Roles** and select **Clone** from the drop-down menu to the right of the required role.
2. Provide a **Name** for the role.
3. Click **Submit** to clone the role.
4. Click the name of the cloned role and navigate to **Filters**.
5. Edit the permissions as required.
6. Click **Submit** to save your new role.

5.3.3. Adding Permissions to a Role

Use the Satellite web UI to add permissions to a role.

Procedure

1. Navigate to **Administer** > **Roles**.
2. Select **Add Filter** from the drop-down list to the right of the required role.
3. Select the **Resource type** from the drop-down list. The *(Miscellaneous)* group gathers permissions that are not associated with any resource group.
4. Click the permissions you want to select from the **Permission** list.
5. Depending on the **Resource type** selected, you can select or deselect the **Unlimited** and **Override** check box. The **Unlimited** checkbox is selected by default, which means that the permission is applied on all resources of the selected type. When you disable the **Unlimited** check box, the **Search** field activates. In this field you can specify further filtering with use of the Red Hat Satellite 6 search syntax. See Section 5.4, "Granular Permission Filtering" for details. When you enable the **Override** check box, you can add additional locations and organizations to allow the role to access the resource type in the additional locations and organizations; you can also remove an already associated location and organization from the resource type to restrict access.
6. Click **Next**.
7. Click **Submit** to save changes.

5.3.4. Viewing Permissions of a Role

Use the Satellite web UI to view the permissions of a role.

Procedure

1. Navigate to **Administer** > **Roles**.
2. Click **Filters** to the right of the required role to get to the **Filters** page.

The **Filters** page contains a table of permissions assigned to a role grouped by the resource type. It is also possible to generate a complete table of permissions and actions that you can use on your Satellite system. See Section 5.3.5, “Creating a Complete Permission Table” for instructions.

5.3.5. Creating a Complete Permission Table

Use the Satellite CLI to create a permission table.

Procedure

1. Ensure that the required packages are installed. Execute the following command on the Satellite Server:

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

2. Start the Satellite console with the following command:

```
# foreman-rake console
```

Insert the following code into the console:

```
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)
```

The above syntax creates a table of permissions and saves it to the **/tmp/table.html** file.

3. Press **Ctrl** + **D** to exit the Satellite console. Insert the following text at the first line of **/tmp/table.html**:

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

Append the following text at the end of **/tmp/table.html**:

```
</table>
```

4. Open **/tmp/table.html** in a web browser to view the table.

5.3.6. Removing a Role

Use the Satellite web UI to remove a role.

Procedure

1. Navigate to **Administer** > **Roles**.
2. Select **Delete** from the drop-down list to the right of the role to be deleted.
3. In an alert box that appears, click **OK** to delete the role.

5.3.7. Predefined Roles Available in Satellite

Role	Permissions Provided by Role [a]
Access Insights Admin	Add and edit Insights rules.
Access Insights Viewer	View Insight reports.
Bookmarks manager	Create, edit, and delete bookmarks.
Boot disk access	Download the boot disk.
Compliance manager	View, create, edit, and destroy SCAP content files, compliance policies, and tailoring files. View compliance reports.
Compliance viewer	View compliance reports.
Create ARF report	Create compliance reports.
Default role	The set of permissions that every user is granted, irrespective of any other roles.
Discovery Manager	View, provision, edit, and destroy discovered hosts and manage discovery rules.
Discovery Reader	View hosts and discovery rules.
Edit hosts	View, create, edit, destroy, and build hosts.
Edit partition tables	View, create, edit and destroy partition tables.
Manager	A role similar to administrator, but does not have permissions to edit global settings. In the Satellite web UI, global settings can be found under **Administer** > **Settings**.
Organization admin	An administrator role defined per organization. The role has no visibility into resources in other organizations.
Red Hat Access Logs	View the log viewer and the logs.

Role	Permissions Provided by Role [a]
Remote Execution Manager	A role with full remote execution permissions, including modifying job templates.
Remote Execution User	Run remote execution jobs.
Site manager	A restrained version of the Manager role.
Tasks manager	View and edit Satellite tasks.
Tasks reader	A role that can only view Satellite tasks.
Viewer	A passive role that provides the ability to view the configuration of every element of the Satellite structure, logs, reports, and statistics.
View hosts	A role that can only view hosts.
Virt-who Manager	A role with full virt-who permissions.
Virt-who Reporter	Upload reports generated by virt-who to Satellite. It can be used if you configure virt-who manually and require a user role that has limited virt-who permissions.
Virt-who Viewer	View virt-who configurations. Users with this role can deploy virt-who instances using existing virt-who configurations.

[a] The exact set of allowed actions associated with predefined roles can be viewed by the privileged user as described in Section 5.3.4, “Viewing Permissions of a Role”

5.4. GRANULAR PERMISSION FILTERING

5.4.1. Granular Permission Filter

As mentioned in Section 5.3.3, “Adding Permissions to a Role” , Red Hat Satellite provides the ability to limit the configured user permissions to selected instances of a resource type. These granular filters are queries to the Satellite database and are supported by the majority of resource types.

5.4.2. Creating a Granular Permission Filter

Create a granular filter using the Satellite UI.

Procedure

- Specify a query in the **Search** field on the **Edit Filter** page. Deselect the **Unlimited** check box for the field to be active. Queries have the following form:

  > *field_name operator value*

Where:

- *field_name* marks the field to be queried. The range of available field names depends on the resource type. For example, the *Partition Table* resource type offers *family*, *layout*, and *name* as query parameters.
- *operator* specifies the type of comparison between *field_name* and *value*. See Section 5.4.4, “Supported Operators for Granular Search” for an overview of applicable operators.
- *value* is the value used for filtering. This can be for example a name of an organization. Two types of wildcard characters are supported: underscore (_) provides single character replacement, while percent sign (%) replaces zero or more characters.

For most resource types, the **Search** field provides a drop-down list suggesting the available parameters. This list appears after placing the cursor in the search field. For many resource types, you can combine queries using logical operators such as *and*, *not* and *has* operators.

> **NOTE**
>
> Satellite does not apply search conditions to create actions. For example, limiting the *create_locations* action with *name = "Default Location"* expression in the search field does not prevent the user from assigning a custom name to the newly created location.

5.4.3. Examples of Using Granular Permission Filters

As an administrator, you can allow selected users to make changes in a certain part of the environment path. The following filter allows you to work with content while it is in the development stage of the application life cycle, but the content becomes inaccessible once is pushed to production.

5.4.3.1. Applying Permissions for the Host Resource Type

The following query applies any permissions specified for the Host resource type only to hosts in the group named host-editors.

```
hostgroup = host-editors
```

The following query returns records where the name matches *XXXX*, *Yyyy*, or *zzzz* example strings:

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

You can also limit permissions to a selected environment. To do so, specify the environment name in the **Search** field, for example:

```
Dev
```

You can limit user permissions to a certain organization or location with the use of the granular permission filter in the **Search** field. However, some resource types provide a GUI alternative, an **Override** check box that provides the **Locations** and **Organizations** tabs. On these tabs, you can select from the list of available organizations and locations. See Section 5.4.3.2, “Creating an Organization Specific Manager Role”.

5.4.3.2. Creating an Organization Specific Manager Role

Use the Satellite UI to create an administrative role restricted to a single organization named *org-1*.

Procedure

1. Navigate to **Administer** > **Roles**.
2. Clone the existing **Organization admin** role. Select **Clone** from the drop-down list next to the **Filters** button. You are then prompted to insert a name for the cloned role, for example *org-1 admin*.
3. Click the desired locations and organizations to associate them with the role.
4. Click **Submit** to create the role.
5. Click *org-1 admin*, and click **Filters** to view all associated filters. The default filters work for most use cases. However, you can optionally click **Edit** to change the properties for each filter. For some filters, you can enable the **Override** option if you want the role to be able to access resources in additional locations and organizations. For example, by selecting the **Domain** resource type, the **Override** option, and then additional locations and organizations using the **Locations** and **Organizations** tabs, you allow this role to access domains in the additional locations and organizations that is not associated with this role. You can also click **New filter** to associate new filters with this role.

5.4.4. Supported Operators for Granular Search

Table 5.1. Logical Operators

Operator	Description
and	Combines search criteria.
not	Negates an expression.
has	Object must have a specified property.

Table 5.2. Symbolic Operators

Operator	Description
=	*Is equal to*. An equality comparison that is case-sensitive for text fields.
!=	*Is not equal to*. An inversion of the = operator.
~	*Like*. A case-insensitive occurrence search for text fields.
!~	*Not like*. An inversion of the ~ operator.
^	*In*. An equality comparison that is case-sensitive search for text fields. This generates a different SQL query to the *Is equal to* comparison, and is more efficient for multiple value comparison.
!^	*Not in*. An inversion of the ^ operator.

>, >=	*Greater than*, *greater than or equal to*. Supported for numerical fields only.
<, ⇐	*Less than*, *less than or equal to*. Supported for numerical fields only.

CHAPTER 6. MANAGING SECURITY COMPLIANCE

Security compliance management is the ongoing process of defining security policies, auditing for compliance with those policies and resolving instances of non-compliance. Any non-compliance is managed according to the organization’s configuration management policies. Security policies range in scope from host-specific to industry-wide, therefore, flexibility in their definition is required.

6.1. SECURITY CONTENT AUTOMATION PROTOCOL

Satellite 6 uses the Security Content Automation Protocol (SCAP) to define security configuration policies. For example, a security policy might specify that for hosts running Red Hat Enterprise Linux, login via SSH is not permitted for the **root** account. With Satellite 6 you can schedule compliance auditing and reporting on all hosts under management. For more information about SCAP, see the Red Hat Enterprise Linux 7 Security Guide.

6.1.1. SCAP Content

SCAP content is a datastream format containing the configuration and security baseline against which hosts are checked. Checklists are described in the extensible checklist configuration description format (XCCDF) and vulnerabilities in the open vulnerability and assessment language (OVAL). Checklist items, also known as rules express the desired configuration of a system item. For example, you may specify that no one can log in to a host over SSH using the **root** user account. Rules can be grouped into one or more profiles, allowing multiple profiles to share a rule. SCAP content consists of both rules and profiles.

You can either create SCAP content or obtain it from a vendor. Supported profiles are provided for Red Hat Enterprise Linux in the scap-security-guide package. The creation of SCAP content is outside the scope of this guide, but see the Red Hat Enterprise Linux 7 Security Guide for information on how to download, deploy, modify, and create your own content.

The default SCAP content provided with the OpenSCAP components of Satellite 6 depends on the version of Red Hat Enterprise Linux. On Red Hat Enterprise Linux 7, content for both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 is installed.

6.1.2. XCCDF Profile

An XCCDF profile is a checklist against which a host or host group is evaluated. Profiles are created to verify compliance with an industry standard or custom standard.

The profiles provided with Satellite 6 are obtained from the OpenSCAP project.

6.1.2.1. Listing Available XCCDF Profiles

In the Satellite UI, list the available XCCD profiles.

Procedure

- Navigate to **Hosts** > **SCAP contents**.

6.2. CONFIGURING SCAP CONTENT

6.2.1. Importing OpenSCAP Puppet Modules

To import the OpenSCAP content into a Puppet environment, you must associate each host that you want to audit with the Puppet environment in the Satellite UI.

Procedure

1. Navigate to **Configure** > **Environments**.
2. Click **Import environments from** ***satellite.example.com***.
3. Select the Puppet environment check box associated with the host you want to audit.
   If no Puppet environment exists, select the **production** environment check box.
4. Click **Update**.

6.2.2. Loading the Default OpenSCAP Content

In the CLI, load the default OpenScap content.

Procedure

- Use the **foreman-rake** command:

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

6.2.3. Extra SCAP Content

You can upload extra SCAP content into the Satellite Server, either content created by yourself or obtained elsewhere. SCAP content must be imported into the Satellite Server before being applied in a policy. For example, the **scap-security-guide** RPM package available in the Red Hat Enterprise Linux 7.2 repositories includes a profile for the Payment Card Industry Data Security Standard (PCI-DSS) version 3. You can upload this content into a Satellite Server even if it is not running Red Hat Enterprise Linux 7.2 as the content is not specific to an operating system version.

6.2.3.1. Uploading Extra SCAP Content

In the Satellite web UI, upload the extra SCAP content.

Procedure

1. Navigate to **Hosts** > **SCAP contents** and click **New SCAP Content**.
2. Enter a title in the **Title** text box.
   Example: **RHEL 7.2 SCAP Content**.
3. Click **Choose file**, navigate to the location containing the SCAP content file and select **Open**.
4. Click **Submit**.

If the SCAP content file is loaded successfully, a message similar to **Successfully created RHEL 7.2 SCAP Content** is shown and the list of **SCAP Contents** includes the new title.

6.3. MANAGING COMPLIANCE POLICIES

6.3.1. Compliance Policy

A scheduled audit, also known as a *compliance policy*, is a scheduled task that checks the specified hosts for compliance against an XCCDF profile. The schedule for scans is specified by the Satellite Server and the scans are performed on the host. When a scan completes, an *Asset Reporting File* (ARF) is generated in XML format and uploaded to the Satellite Server. You can see the results of the scan in the compliance policy dashboard. No changes are made to the scanned host by the compliance policy. The SCAP content includes several profiles with associated rules but policies are not included by default.

6.3.2. Creating a Compliance Policy

In the Satellite web UI, create a compliance policy to scan your content hosts for security compliance.

Prerequisite

- Each host that you want to audit is associated with a Puppet environment.
  For more information, see Section 6.2.1, “Importing OpenSCAP Puppet Modules” .

Procedure

1. Navigate to **Hosts** > **Policies**, click **New Policy** and follow the wizard’s steps.
2. Enter a name for this policy, a description (optional), then click **Next**.
3. Select the SCAP Content and XCCDF Profile to be applied, then click **Next**.
   Until BZ#1704582 is resolved, note that the **Default XCCDF Profile** might return an empty report.
4. Specify the scheduled time when the policy is to be applied, then click **Next**.
   Select **Weekly**, **Monthly**, or **Custom** from the **Period** drop-down list.
   - If you select **Weekly**, also select the desired day of the week from the **Weekday** drop-down list.
   - If you select **Monthly**, also specify the desired day of the month in the **Day of month** field.
   - If you select **Custom**, enter a valid Cron expression in the **Cron line** field.
     The **Custom** option allows for greater flexibility in the policy’s schedule than either the **Weekly** or **Monthly** options.
5. Select the locations to which the policy is to be applied, then click **Next**.
6. Select the organizations to which the policy is to be applied, then click **Next**.
7. Select the host groups to which the policy is to be applied, then click **Submit**.

When the Puppet agent runs on the hosts which belong to the selected host group, or hosts to which the policy has been applied, the OpenSCAP client will be installed and a Cron job added with the policy’s specified schedule. The **SCAP Content** tab provides the name of the SCAP content file which will be distributed to the directory **/var/lib/openscap/content/** on all target hosts.

6.3.3. Viewing a Compliance Policy

You can preview the rules which will be applied by specific OpenSCAP content and profile combination. This is useful when planning policies.

In the Satellite web UI, view the compliance policy.

Procedure

1. Navigate to **Hosts** > **Policies**.
2. Click **Show Guide**.

6.3.4. Editing a Compliance Policy

In the Satellite web UI, edit the compliance policy.

Procedure

1. Navigate to **Hosts** > **Policies**.
2. From the drop-down list to the right of the policy's name, select **Edit**.
3. Edit the necessary attributes.
4. Click **Submit**.

An edited policy is applied to the host when its Puppet agent next checks with the Satellite Server for updates. By default this occurs every 30 minutes.

6.3.5. Deleting a Compliance Policy

In the Satellite web UI, delete an existing policy.

1. Navigate to **Hosts** > **Policies**.
2. From the drop-down list to the right of the policy's name, select **Delete**.
3. Click **OK** in the confirmation message.

6.3.6. Adding a Compliance Policy to Hosts

You must add a policy to a host, or a host group, which you want to scan for security compliance.

In the Satellite web UI, add a policy to one or more hosts.

1. Navigate to **Hosts** > **All hosts**.
2. Select the host or hosts to which you want to add the policy.
3. Click **Select Action**.
4. Select **Assign Compliance Policy** from the list.
5. In the new panel that opens, select the appropriate policy from the list of available policies and click **Submit**.

6.4. TAILORING FILES

Tailoring Files allow existing OpenSCAP policies to be customized without forking or rewriting the policy. You can assign a Tailoring File to a policy when creating or updating a policy.

You can create a Tailoring File using the SCAP Workbench. For more information on using the SCAP Workbench tool, see Customizing SCAP Security Guide for your use-case .

6.4.1. Uploading a Tailoring File

In the Satellite web UI, upload a Tailoring file.

Procedure

1. Navigate to **Hosts** > **Compliance - Tailoring Files**and click **New Tailoring File**.
2. Enter a name in the **Name** text box.
3. Click **Choose File**, navigate to the location containing the SCAP DataStream Tailoring File and select **Open**.
4. Click **Submit** to upload the chosen Tailoring File.

6.4.2. Assigning a Tailoring File to a Policy

In the Satellite web UI, assign a Tailoring file to a policy.

Procedure

1. Navigate to **Hosts** > **Compliance - Policies**.
2. Click **New Policy**, or **New Compliance Policy** if there are existing Compliance Policies.
3. Enter a name in the **Name** text box, and click **Next**.
4. Select a **Scap content** from the dropdown menu.
5. Select a **XCCDF Profile** from the dropdown menu.
6. Select a **Tailoring File** from the dropdown menu.
7. Select a **XCCDF Profile in Tailoring File**from the dropdown menu.
   It is important to select the XCCDF Profile because Tailoring Files are able to contain multiple XCCDF Profiles.
8. Click **Next**.
9. Select a **Period** from the dropdown menu.
10. Select a **Weekday** from the dropdown menu, and click **Next**.
11. Select a **Location** to move it to the **Selected Items** window, and click **Next**.
12. Select an **Organization** to move it to the **Selected Items** window, and click **Next**.
13. Select a **Hostgroup** to move it to the **Selected Items** window, and click **Submit**.

6.5. MONITORING COMPLIANCE

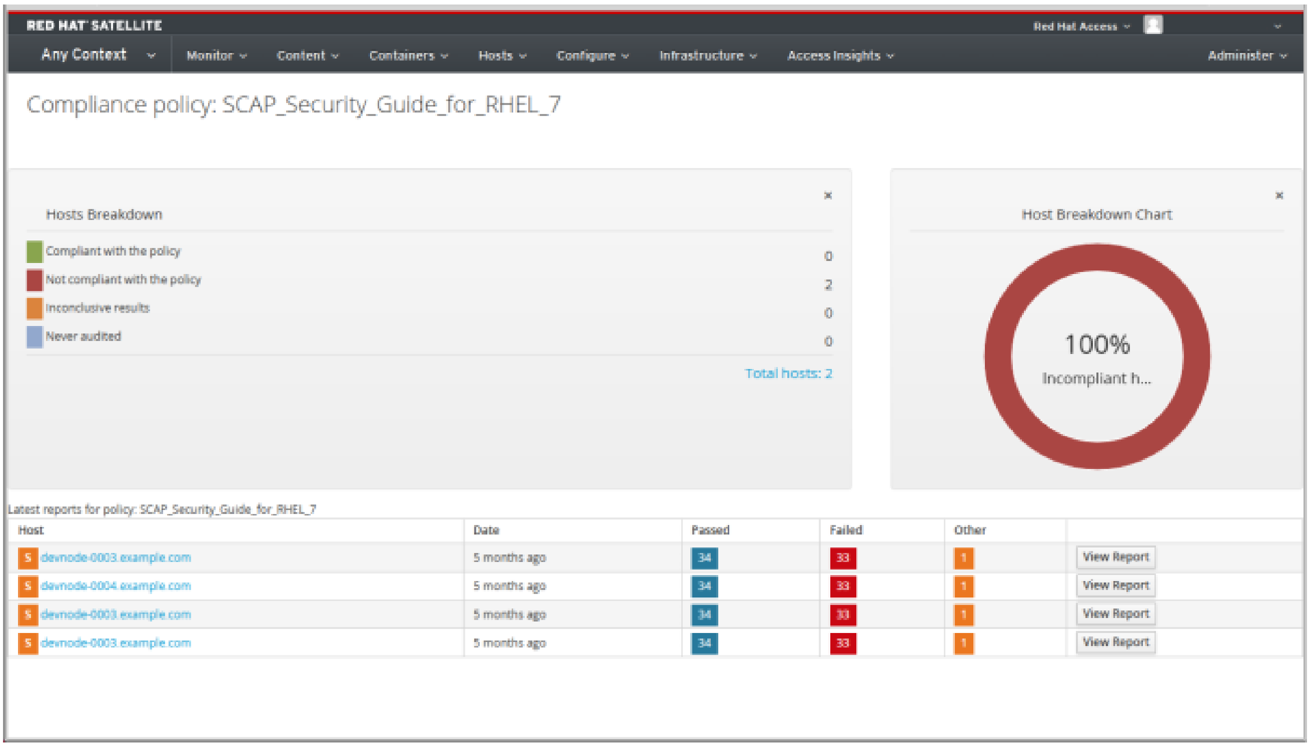
Red Hat Satellite 6 enables centralized compliance monitoring and management. A compliance dashboard provides an overview of compliance of hosts and the ability to view details for each host within the scope of that policy. Compliance reports provide a detailed analysis of compliance of each host with the applicable policy. With this information, you can evaluate the risks presented by each host and manage the resources required to bring hosts into compliance.

Common objectives when monitoring compliance using SCAP include the following:

- Verifying policy compliance.
- Detecting changes in compliance.

6.5.1. Compliance Policy Dashboard

The compliance policy dashboard provides a statistical summary of compliance of hosts and the ability to view details for each host within the scope of that policy. For all hosts which were evaluated as non-compliant, the **Failed** statistic provides a useful metric for prioritizing compliance effort. The hosts detected as **Never audited** should also be a priority, since their status is unknown.



Compliance policy: SCAP_Security_Guide_for_RHEL_7

Hosts Breakdown

🟩 Compliant with the policy	0
🟥 Not compliant with the policy	2
🟧 Inconclusive results	0
🟦 Never audited	0

Total hosts: 2

Latest reports for policy: SCAP_Security_Guide_for_RHEL_7

Host	Date	Passed	Failed	Other	
S devnode-0003.example.com	5 months ago	34	33	1	View Report
S devnode-0004.example.com	5 months ago	34	33	1	View Report
S devnode-0003.example.com	5 months ago	34	33	1	View Report
S devnode-0003.example.com	5 months ago	34	33	1	View Report

6.5.2. Viewing the Compliance Policy Dashboard

Use the Satellite web UI to verify policy compliance with the compliance policy dashboard.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Policies**.
2. Click the required policy name. The dashboard provides the following information:
   - A ring chart illustrating a high-level view of compliance of hosts with the policy.
   - A statistical breakdown of compliance of hosts with the policy, in a tabular format.

- Links to the latest policy report for each host.

6.5.3. Compliance Email Notifications

The Satellite Server sends an OpenSCAP Summary email to all users who subscribe to the **Openscap policy summary** email notifications. For more information on subscribing to email notifications, see Section 5.1.6, "Configuring Email Notifications". Each time a policy is run, Satellite checks the results against the previous run, noting any changes between them. The email is sent according to the frequency requested by each subscriber, providing a summary of each policy and its most recent result.

An **OpenSCAP Summary** email message contains the following information:

- Details of the time period it covers.
- Totals for all hosts by status: changed, compliant, and noncompliant.
- A tabular breakdown of each host and the result of its latest policy, including totals of the rules that passed, failed, changed, or where results were unknown.

6.5.4. Compliance Report

A compliance report is the output of a policy run against a host. Each report includes the total number of rules passed or failed per policy. By default, reports are listed in descending date order.

In the Satellite web UI, navigate to **Hosts** > **Reports** to list all compliance reports.

A compliance report consists of the following areas:

- Introduction
- Evaluation Characteristics
- Compliance and Scoring
- Rule Overview

Evaluation Characteristics

The Evaluation Characteristics area provides details about an evaluation against a specific profile, including the host that was evaluated, the profile used in the evaluation, and when the evaluation started and finished. For reference, the IPv4, IPv6, and MAC addresses of the host are also listed.

Name	Description	Example
Target machine	The fully-qualified domain name (FQDN) of the evaluated host.	**test-system.example.com**
Benchmark URL	The URL of the SCAP content against which the host was evaluated.	**/var/lib/openscap/content/1fbdc87d24db51ca184419a2b6f**
Benchmark ID	The identifier of the benchmark against which the host was evaluated. A benchmark is a set of profiles	**xccdf_org.ssgproject.content_benchmark_RHEL_7**

Name	Description	Example
Profile ID	The identifier of the profile against which the host was evaluated.	**xccdf_org.ssgproject_content_profile_rht-ccp**
Started at	The date and time at which the evaluation started, in ISO 8601 format.	**2015-09-12T14:40:02**
Finished at	The date and time at which the evaluation finished, in ISO 8601 format.	**2015-09-12T14:40:05**
Performed by	The local account name under which the evaluation was performed on the host.	**root**

Compliance and Scoring

The Compliance and Scoring area provides an overview of whether or not the host is in compliance with the profile rules, a breakdown of compliance failures by severity, and an overall compliance score as a percentage. If compliance with a rule was not checked, this is categorized in the **Rule results** field as **Other**.

Rule Overview

The Rule Overview area provides details about every rule and the compliance result, with the rules presented in a hierarchical layout.

Select or clear the check boxes to narrow the list of rules included in the compliance report. For example, if the focus of your review is any non-compliance, clear the **pass** and **informational** check boxes.

To search all rules, enter a criterion in the **Search** field. The search is dynamically applied as you type. The **Search** field only accepts a single plain-text search term and it is applied as a case-insensitive search. When you perform a search, only those rules whose descriptions match the search criterion will be listed. To remove the search filter, delete the search criterion.

For an explanation of each result, hover the cursor over the status shown in the **Result** column.

6.5.5. Examining Compliance Failure of Hosts

Use the Satellite web UI to determine why a host failed compliance on a rule.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Reports** to list all compliance reports.
2. Click **View Report** in the row of the specific host to view the details of an individual report.
3. Click on the rule’s title to see further details:
    - A description of the rule with instructions for bringing the host into compliance if available.
    - The rationale for the rule.

- In some cases, a remediation script.

> **WARNING**
>
> Do not implement any of the recommended remedial actions or scripts without first testing them in a non-production environment.

6.5.6. Searching Compliance Reports

Use the Compliance Reports search field to narrow down the list of available reports on any given subset of hosts.

Procedure

- To apply a filter, enter the search criteria in the **Search** field and click **Search**. The performed search is case-insensitive.

Search Use Cases

- The following search criteria finds all compliance reports for which more than five rules failed:

  ```
  failed > 5
  ```

- The following search criteria finds all compliance reports created after January 1, *YYYY*, for hosts with host names that contain the **prod-** group of characters:

  ```
  host ~ prod- AND date > "Jan 1, YYYY"
  ```

- The following search criteria finds all reports generated by the **rhel7_audit** compliance policy from an hour ago:

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

Additional Information

- To see a list of available search parameters, click on the empty **Search** field.

- You can create complex queries with the following logical operators: **and**, **not** and **has**. For more information about logical operators, see Section 5.4.4, “Supported Operators for Granular Search”.

- Regular expressions are not valid search criteria, however, you can use multiple fields in a single search expression. For more information about all available search operators, see Section 5.4.4, “Supported Operators for Granular Search”.

- You can bookmark a search to reuse the same search criteria. For more information, see Section 16.3.1, “Creating Bookmarks”.

6.5.7. Deleting a Compliance Report

To delete a compliance report, complete the following steps:

1. In the Satellite web UI, navigate to **Hosts** > **Reports**.
2. In the Compliance Reports window, identify the policy that you want to delete and, on the right of the policy's name, select **Delete**.
3. Click **OK**.

6.5.8. Deleting Multiple Compliance Reports

You can delete multiple compliance policies simultaneously. However, in the Satellite web UI, compliance policies are paginated, so you must delete one page of reports at a time. If you want to delete all OpenSCAP reports, use the script in the Deleting OpenSCAP Reports section of the *Red Hat Satellite API Guide*

1. In the Satellite web UI, navigate to **Hosts** > **Reports**.
2. In the Compliance Reports window, select the compliance reports that you want to delete.
3. In the upper right of the list, select **Delete reports**.
4. Repeat these steps for as many pages as you want to delete.

6.6. SPECIFICATIONS SUPPORTED BY OPENSCAP

The following specifications are supported by OpenSCAP:

Title	Description	Version
XCCDF	The 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

CHAPTER 7. DISABLING WEAK ENCRYPTION

You might want to change the encryption settings for Satellite depending on the security requirements of your infrastructure or to fix vulnerabilities quickly. Use the following sections to disable weak SSL encryption and 64-bit cipher suites.

7.1. DISABLING WEAK SSL 2.0 AND SSL 3.0 ENCRYPTION

If your Satellite fails Nessus scans because of SSL vulnerabilities, or your security infrastructure requires that you disable SSL 2.0 and SSL 3.0, you can edit the **/etc/foreman-installer/custom-hiera.yaml** file to remove weak encryption.

Disabling Weak SSL 2.0 and SSL 3.0 Encryption for Satellite

To disable weak encryption for Satellite, complete the following steps:

1. Open the **/etc/foreman-installer/custom-hiera.yaml** file for editing:

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

2. Add the following entries:

```
# 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. Rerun the **satellite-installer** tool with no arguments:

```
# satellite-installer --scenario satellite
```

4. Restart Katello services:

```
# katello-service restart
```

Disabling Weak SSL 2.0 and SSL 3.0 Encryption for Capsule

To disable weak encryption for Capsule, complete the following steps:

1. Open the **/etc/foreman-installer/custom-hiera.yaml** file for editing:

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

2. Add the following entries:

```
# 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. Rerun the **satellite-installer** tool with no arguments:

```
# satellite-installer --scenario capsule
```

4. Restart Katello services:

```
# katello-service restart
```

7.2. DISABLING 64-BIT BLOCK SIZE CIPHER SUITES (SWEET32)

If you want to update your cipher suites for Satellite, you can edit the ciphers and then add your changes to the **/etc/foreman-installer/custom-hiera.yaml** file to make these changes persistent.

You can use the following procedure to update your cipher suite.

Until BZ#1586271 is resolved, you might want to disable SSL 64-bit Block Size Cipher Suites (SWEET32). However, you can also use this procedure to update other ciphers and make these changes persistent.

The minimum browser requirements for the following Ciphers is Firefox 27.

1. Open the **/etc/httpd/conf.d/ssl.conf** Apache configuration file for editing:

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

2. Update the values of **SSLCipherSuite** parameter:

```
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. Restart the **httpd** service:

```
# systemctl restart httpd
```

4. To make the change persistent across different satellite-installer executions, open the **/etc/foreman-installer/custom-hiera.yaml** file for editing:

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

5. Add the following entry for **apache**:

```
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
```

6. Run the **satellite-installer** tool to add the changes to the Apache configuration:

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

CHAPTER 8. BACKING UP SATELLITE SERVER AND CAPSULE SERVER

This chapter describes the minimum backup procedure to ensure the continuity of your Red Hat Satellite deployment and associated data in the event of a disaster. If your deployment uses custom configurations, you must consider how to handle these custom configurations when you plan your backup and disaster recovery policy.

8.1. BACKING UP SATELLITE SERVER OR CAPSULE SERVER

Use this section to create a backup of your Satellite Server or Capsule Server and all associated data using the **foreman-maintain backup** script. Backing up to a separate storage device on a separate system is highly recommended. Satellite services are unavailable during the backup. The backup can be scheduled for a quiet time using **cron**, see the A Weekly Full Backup Followed by Daily Incremental Backups.

During offline or snapshot backups, the services are inactive and Satellite is in a maintenance mode. All the traffic from outside on port 443 is rejected by a firewall to ensure there are no modifications triggered.

A backup contains sensitive information from the **/root/ssl-build** directory. For example, it can contain hostnames, ssh keys, request files and SSL certificates. Either encrypt or move the backup to a secure location to minimize the risk of damage or unauthorized access to the hosts.

Prerequisites

Ensure that no other tasks are scheduled by other administrators for the same time. This is particularly important when administrators are working in different locations and time zones.

Conventional Backup Methods

You can also use conventional backup methods such as that described in the System Backup and Recovery section of the *Red Hat Enterprise Linux 7 System Administrator's Guide*. When creating a snapshot or conventional backup, stop all services. Do not do this if using the **foreman-maintain backup** script:

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

Start the services after creating a snapshot or conventional backup:

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

8.1.1. Estimating the size of a Backup

The full backup creates uncompressed archives of MongoDB, PostgreSQL, and Pulp database files and Satellite configuration files. Compression occurs after the archives are created to decrease the time when Satellite services are unavailable. Consequently, a full backup requires space to store the following data:

- Uncompressed Satellite databases and configuration files.
- Compressed Satellite databases and configuration files.
- An extra 20% of the total estimated space to ensure a reliable backup.

To Estimate the Size of a Backup

1. Enter the **du** command to estimate the size of uncompressed directories containing Satellite databases and configuration files:

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

2. Calculate how much space is required to store the compressed data.
   Table 8.1, "Backup Data Compression Ratio" demonstrates compression ratio of all data items used in the backup.

   Table 8.1. Backup Data Compression Ratio

Data type	Directory	Ratio	Example results
MongoDB database files	**/var/lib/mongodb**	85 - 90 %	480 GB → 60 GB
PostgreSQL database files	**/var/lib/pgsql/data**	80 - 85%	100 GB → 20 GB
Pulp RPM files	**/var/lib/pulp**	(not compressed)	100 GB
Configuration files	**/var/lib/qpidd** **/var/lib/tftpboot** **/etc** **/root-ssl/build** **/var/www/html/pub** **/opt/puppetlabs**	85%	942 MB → 141 MB

   In this example, the compressed backup data occupies 180 GB in total.

3. To calculate how much space you need to store a backup, add the total of the estimated values of compressed and uncompressed backup data and then add an extra 20% to ensure a reliable backup.
   This example requires 681 GB plus 180 GB for the uncompressed and compressed backup data, 861 GB in total. With 172 GB of extra space, 1033 GB must be allocated for the backup location.

8.1.2. Performing a Full Backup of Satellite Server or Capsule Server

Red Hat Satellite 6.4 uses the **foreman-maintain backup** script to make backups. To see the usage statement, enter the following command:

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

There are three main methods of backing up Satellite Server:

- Offline backup
- Online backup
- Snapshot backups
  For more information about each of these methods, you can view the usage statements for each script.

For offline backups:

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

For online backups:

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

For backups from snapshots:

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

Directory creation

The **foreman-maintain backup** script creates a time-stamped subdirectory in the backup directory you specify. The **foreman-maintain backup** script does not overwrite backups. You must select the correct directory or subdirectory when restoring from a backup or an incremental backup. The script stops and restarts services as required.

If you must set the directory name yourself add the **--preserve-directory** option and add a directory name. The backup is then stored in the directory you provide on the command line.

If you use **--preserve-directory**, no data is removed if the backup fails.

Note that user **postgres** needs write access to that directory if you have a local PgSQL database.

Remote databases

You can use the **foreman-maintain backup** script to back up remote databases.

You can use both online and offline methods to back up remote databases, but if you use offline methods, such as snapshot, the **foreman-maintain backup** script performs a database dump.

To Perform a Full Offline Backup of Satellite Server or Capsule Server:

Use this procedure to perform a full offline backup. Satellite services are unavailable during the backup process.

> **WARNING**
>
> Request other users of Satellite Server or Capsule Server to save any changes and warn them that Satellite services are unavailable for the duration of the backup. Ensure no other tasks are scheduled for the same time as the backup.

1. Ensure that your backup location has enough disk space to store the backup. For more information, see Section 8.1.1, “Estimating the size of a Backup” .
2. Run the backup script:

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

   This process can take a long time to complete, because of the amount of data to copy.

8.1.3. Performing a Backup without Pulp Content

To Perform a Backup without Pulp Content:

Use this procedure to perform an offline backup but excludes the contents of the Pulp directory. This backup is useful for debugging purposes and is only intended to provide access to configuration files without spending time backing up the Pulp database. You cannot restore from a directory that does not contain Pulp content.

> **WARNING**
>
> Request other users of Satellite Server or Capsule Server to save any changes and warn them that Satellite services are unavailable for the duration of the backup. Ensure no other tasks are scheduled for the same time as the backup.

1. Ensure that your backup location has enough disk space to store the backup. For more information, see Section 8.1.1, “Estimating the size of a Backup” .
2. Run the backup script:

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

8.1.4. Performing an Incremental Backup

To Perform an Incremental Backup:

Use this procedure to perform an offline backup of any changes since a previous backup. Use a full backup as a reference to make the first incremental backup of a sequence. Keep at least the last known good full backup and a complete sequence of incremental backups to restore from.

> **WARNING**
>
> Request other users of Satellite Server or Capsule Server to save any changes and warn them that Satellite services are unavailable for the duration of the backup. Ensure no other tasks are scheduled for the same time as the backup.

1. Ensure your backup location has enough disk space to store the backup. For more information, see Section 8.1.1, "Estimating the size of a Backup" .

2. Create a full backup:

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

3. Run the backup script with the **--incremental** argument. This creates a directory within your backup directory to store the first incremental back up.

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

4. Run the backup script again to create the second incremental backup. Point to your first incremental backup to indicate the starting point for the next increment. This creates a directory for the second incremental backup in your backup directory.

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

   If you want to point to a different version of the backup, and make a series of increments with that version of the backup as the starting point, you can do this at any time. For example, if you want to make a new incremental backup from the full backup rather than the first or second incremental backup, point to the full backup directory:

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

8.1.5. Example of a Weekly Full Backup Followed by Daily Incremental Backups

A Weekly Full Backup Followed by Daily Incremental Backups

The script makes a full backup on a Sunday and incremental backups of the following days. Each day that a backup is made, a new subdirectory is created. This script requires a daily cron job.

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

```
  foreman-maintain backup offline --assumeyes --incremental "$LAST" $DESTINATION
fi
exit 0
```

Note that the **foreman-maintain backup** script requires **/sbin** and **/usr/sbin** directories to be in **PATH**, and the **--assumeyes** option, because the command prompts for confirmation for the backup to proceed.

8.1.6. Performing an Online Backup

Perform an online backup only for debugging purposes. If there are procedures affecting the Pulp database, the Pulp part of the backup procedure repeats until it is no longer being altered. Because the backup of the Pulp database is the most time consuming part of backing up Satellite, if you make a change that alters the Pulp database during this time, the backup procedure keeps restarting.

Risks Associated with Online Backups

Data mismatches can occur between Mongo and Postgres databases while the services are online.

When performing an online backup, if there are procedures affecting the Pulp database, the Pulp part of the backup procedure repeats until it is no longer being altered. Because the backup of the Pulp database is the most time consuming part of backing up Satellite, if you make a change that alters the Pulp database during this time, the backup procedure keeps restarting.

For production environments, use the snapshot method. For more information, see Section 8.1.7, “Performing a Snapshot Backup”. If you want to use the online backup method in production, proceed with caution and ensure that no modifications occur during the backup.

WARNING

Request other users of Satellite Server or Capsule Server to save any changes and warn them that Satellite services are unavailable for the duration of the backup. Ensure no other tasks are scheduled for the same time as the backup.

To Perform an Online Backup:

1. Ensure that your backup location has enough disk space to store the backup. For more information, see Section 8.1.1, “Estimating the size of a Backup” .

2. Run the backup script:

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

8.1.7. Performing a Snapshot Backup

The snapshot backup method uses Logical Volume Manager (LVM) snapshots of the Pulp, MongoDB, and PostgreSQL directories. The backup is then created from the LVM snapshots and not from the running Satellite as with online backup, which mitigates the risk of creating an inconsistent backup. The snapshot backup method is faster than a full offline backup, which reduces Satellite downtime.

To Perform a Snapshot Backup:

To view the usage statement, enter the following command:

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

Prerequisites

Before you perform the snapshot backup, ensure that the following conditions exist:

- The system uses LVM for the directories that you snapshot: **/var/lib/pulp/**, **/var/lib/mongodb/**, and **/var/lib/pgsql/**.
- The free disk space in the relevant volume group (VG) is three times the size of the snapshot. More precisely, the VG must have enough space unreserved by the member logical volumes (LVs) to accommodate new snapshots. In addition, one of the LVs must have enough free space for the backup directory.
- The target backup directory is on a different LV than the directories that you snapshot.

> **WARNING**
>
> Request other Satellite Server or Capsule Server users to save any changes and warn them that Satellite services are unavailable for the duration of the backup. Ensure no other tasks are scheduled for the same time as the backup.

Run the backup script:

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

The **foreman-maintain backup snapshot** makes snapshots when the services are active, and stops all services which could impact the backup. This makes the maintenance window shorter. After the successful snapshot, all services are restarted and LVM snapshots are removed.

8.1.8. White-listing and Skipping Steps

A backup using the **foreman-maintain backup** script proceeds in a sequence of steps. To skip part of the backup add the **--whitelist** option to the command and add the step label that you want to omit. For example:

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

To see a list of available step labels use:

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

CHAPTER 9. RESTORING SATELLITE SERVER OR CAPSULE SERVER FROM A BACKUP

You can restore Red Hat Satellite Server or Red Hat Capsule Server from the backup data that you create as part of Section 8.1, “Backing up Satellite Server or Capsule Server” . This process outlines how to restore the backup on the same server that generated the backup, and all data covered by the backup is deleted on the target system. If the original system is unavailable, provision a system with the same configuration settings and host name.

9.1. RESTORING FROM A FULL BACKUP

Use this procedure to restore Red Hat Satellite or Capsule Server from a full backup. When the restore process completes, all processes are online, and all databases and system configuration revert to the state at the time of the backup.

Prerequisites

- Ensure that you are restoring to the correct instance. The Red Hat Satellite instance must have the same host name, configuration, and be the same major version as the original system.

- Ensure that you have an existing target directory. The target directory is read from the configuration files contained within the archive.

- Ensure that you have enough space to store this data on the base system of Satellite Server or Capsule Server as well as enough space after the restoration to contain all the data in the /**etc**/ and /**var**/ directories contained within the backup.
  To check the space used by a directory, enter the following command:

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

  To check for free space, enter the following command:

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

  Add the **--total** option to get a total of the results from more than one directory.

- Ensure that all SELinux contexts are correct. Enter the following command to restore the correct SELinux contexts:

  ```
  # restorecon -Rnv /
  ```

Procedure

1. Choose the appropriate method to install Satellite or Capsule:

   - To install Satellite Server from a connected network, follow the procedures in Installing Satellite Server from a Connected Network.

   - To install Satellite Server from a disconnected network, follow the procedures in Installing Satellite Server from a Disconnected Network.

   - To install a Capsule Server, follow the procedures in the Installing Capsule Server.

2. Copy the backup data to Satellite Server’s local file system. Use **/var/** or **/var/tmp/**.

3. Run the restoration script.

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

   Where *backup_directory* is the time-stamped directory or subdirectory containing the backed-up data.

   The restore process can take a long time to complete, because of the amount of data to copy.

Additional Resources

- For troubleshooting, you can check **/var/log/foreman/production.log** and **/var/log/messages**.

9.2. RESTORING FROM INCREMENTAL BACKUPS

Use this procedure to restore Satellite or Capsule Server from incremental backups. If you have multiple branches of incremental backups, select your full backup and each incremental backup for the “branch” you want to restore, in chronological order.

When the restore process completes, all processes are online, and all databases and system configuration revert to the state at the time of the backup.

Procedure

1. Restore the last full backup using the instructions in Section 9.1, “Restoring from a Full Backup” .

2. Remove the full backup data from Satellite Server’s local file system, for example, **/var/** or **/var/tmp/**.

3. Copy the incremental backup data to Satellite Server’s local file system, for example, **/var/** or **/var/tmp/**.

4. Restore the incremental backups in the same sequence that they are made:

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

   If you created the backup using the **foreman-maintain backup** command, you do not need to use **-i** option in the command.

Additional Resources

- For troubleshooting, you can check **/var/log/foreman/production.log** and **/var/log/messages**.

9.3. BACKUP AND RESTORE CAPSULE SERVER USING A VIRTUAL MACHINE SNAPSHOT

If your Capsule Server is a virtual machine, you can restore it from a snapshot. Creating weekly snapshots to restore from is recommended. In the event of failure, you can install, or configure a new Capsule Server, and then synchronize the database content from Satellite Server.

If required, deploy a new Capsule Server, ensuring the host name is the same as before, and then install the Capsule certificates. You may still have them on Satellite Server, the package name ends in -certs.tar, alternately create new ones. Follow the procedures in Installing Capsule Server until you can confirm, in the web UI, that Capsule Server is connected to Satellite Server. Then use the procedure Section 9.3.1, “Synchronizing an External Capsule” to synchronize from Satellite.

9.3.1. Synchronizing an External Capsule

Synchronize an external Capsule with Satellite.

Procedure

1. To synchronize an external Capsule, select the relevant organization and location in the web UI, or choose **Any Organization** and **Any Location**.
2. Navigate to **Infrastructure** > **Capsules** and click the name of the Capsule to synchronize.
3. On the **Overview** tab, select **Synchronize**.

CHAPTER 10. RENAMING A SATELLITE SERVER OR CAPSULE SERVER

Renaming a Satellite Server or Capsule Server requires use of the **satellite-change-hostname** script. Red Hat Satellite contains references to the host's name and these changes are made using the script. Renaming a Satellite Server affects itself, all Capsule Servers and all hosts registered to it. Renaming a Capsule Server affects itself and all hosts registered to it.

> **WARNING**
>
> The renaming process shuts down all Satellite Server services on the host being renamed. When the renaming is complete, all services are restarted.

10.1. RENAMING A SATELLITE SERVER

The host name of a Satellite Server is used by Satellite Server components, all Capsule Servers, and hosts registered to it for communication. Renaming a Satellite Server requires that these references be updated.

If you use external authentication, you must reconfigure Satellite Server for external authentication after you run the **satellite-change-hostname** script. The **satellite-change-hostname** script breaks external authentication for Satellite Server. For more information about configuring external authentication, see Chapter 13, *Configuring External Authentication*

Prerequisites

- (Optional) If the Satellite Server has a custom X.509 certificate installed, a new certificate must be obtained in the host's new name. When all hosts are re-registered to the Satellite Server, the new certificate is installed. For more information on obtaining a custom X.509 certificate, see Configuring Satellite Server with a Custom Server Certificate in *Installing Satellite Server from a Connected Network*.

- Backup the Satellite Server. The **satellite-change-hostname** script makes irreversible changes to the Satellite Server. If the renaming process is not successful, you must restore it from backup. For more information, see Section 13.2, "Using Identity Management" .

Rename a Satellite Server

1. On the Satellite Server, choose the appropriate method to run the **satellite-change-hostname** script, providing the new host name and Satellite credentials:

   - If your Satellite Server is installed with self-signed certificates:

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

   - If your Satellite Server is installed with SSL certificates:

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

The message ***** **Hostname change complete!** ***** confirms that the rename completed successfully.

2. (Optional) If you have obtained a new X.509 certificate for the new Satellite Server host name, run the Satellite installation script to install the certificate. For more information about installing a custom X.509 certificate, see Configuring Satellite Server with a Custom Server Certificate in *Installing Satellite Server from a Connected Network* .

3. On all Capsule Servers and hosts registered to the Satellite Server, reinstall the bootstrap RPM and re-register them to the Satellite Server. Substitute the example organization and environment values with those matching your environment.

   a.

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

   b.

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

   c.

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

   Use of the Red Hat Satellite remote execution feature is recommended for this step. For more information, see Configuring and Running Remote Commands in *Managing Hosts*.

4. Reattach subscriptions to all Capsule Servers and hosts registered to the Satellite Server, then refresh the subscription.

   a.

   ```
   # subscription-manager refresh
   ```

   b.

   ```
   # yum repolist
   ```

   Use of the Red Hat Satellite remote execution feature is recommended for this step. For more information, see Configuring and Running Remote Commands in *Managing Hosts*.

5. On all Capsule Servers, re-run the Satellite installation script to update references to the new host name.

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

6. On the Satellite Server, synchronize content for each Capsule Server.

    a. List all Capsule Servers with their ID numbers:

    ```
    # hammer capsule list
    ```

    b. Enter the following command for each Capsule Server:

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

10.2. RENAMING A CAPSULE SERVER

The host name of a Capsule Server is referenced by Satellite Server components, and all hosts registered to it. Renaming a Capsule Server requires that these references be updated.

Prerequisites

- Optional: New X.509 custom certificate files for the Capsule Server. For more information on obtaining a custom X.509 certificate, see Configuring Capsule Server with a Custom Server Certificate in *Installing Capsule Server* .
- Backup the Capsule Server. The **satellite-change-hostname** script makes irreversible changes to the Capsule Server. If the renaming process is not successful, you must restore it from backup.
  Red Hat Satellite does not provide a native backup method for a Capsule Server. For more information, see Chapter 8, *Backing Up Satellite Server and Capsule Server* .

Renaming a Capsule Server:

1. On Satellite Server, create a new certificates archive file.
    - If you are using the default Satellite Server certificate, enter the following command:

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

      Ensure that you enter the full path to the **.tar** file.
    - If you are using a custom X.509 certificate on the Capsule Server, see Create the Capsule Server's Certificate Archive File in *Installing Capsule Server* .
2. On Satellite Server, copy the certificates archive file to the Capsule Server, providing the **root** user's password when prompted. In this example the archive file is copied to the **root** user's home directory, but you may prefer to copy it elsewhere.

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

3. On the Capsule Server, run the **satellite-change-hostname** script, providing the host's new name, Satellite credentials, and certificates archive filename.

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

Ensure that you enter the full path to the **.tar** file.

The message ***** **Hostname change complete!** ***** confirms that the rename completed successfully.

4. Optional: If you have obtained a new X.509 certificate in the Capsule Server's new host name, run the Satellite installation script to install the certificate. For more information about installing a custom X.509 certificate, see Install the Capsule Server's Custom Certificate in *Installing Capsule Server*.

5. On all hosts registered to the Capsule Server, reinstall the bootstrap RPM and re-register them to the Capsule Server. Substitute the example organization and environment values with those matching your environment.

```
# 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
```

Use of the Red Hat Satellite remote execution feature is recommended for this step. For more information, see Running Jobs on Hosts in *Managing Hosts*.

6. Reattach subscriptions to all hosts registered to the Capsule Server, then refresh the subscription.

```
# subscription-manager refresh
```

```
# yum repolist
```

7. Edit the Capsule Server's name.

   a. In the Satellite web UI, navigate to **Infrastructure** > **Capsules**.

   b. Find the Capsule Server in the list, and click **Edit** in that row.

   c. Edit the **Name** and **URL** fields to match the Capsule Server's new host name, then click **Submit**.

8. On your DNS server, add a record for the Capsule Server's new host name, and delete the record for the previous host name.

CHAPTER 11. MAINTAINING SATELLITE SERVER

This chapter provides information on how to maintain a Red Hat Satellite Server, including information on how to work with audit records, how to clean unused tasks, how to recover Pulp from a full disc, how to reclaim disc space from NongoDB, and how to use Red Hat Insights to proactively diagnose systems.

11.1. DELETING AUDIT RECORDS

Audit records are created automatically in Satellite. You can use the **foreman-rake audits:expire** command to remove audits at any time. You can also use a cron job to schedule audit record deletions at the set interval that you want.

By default, using the **foreman-rake audits:expire** command removes audit records that are older than 90 days. You can specify the number of days to keep the audit records by adding the **days** option and add the number of days.

For example, if you want to delete audit records that are older than seven days, enter the following command:

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

11.2. ANONYMIZING AUDIT RECORDS

You can use the **foreman-rake audits:anonymize** command to remove any user account or IP information while maintaining the audit records in the database. You can also use a cron job to schedule anonymizing the audit records at the set interval that you want.

By default, using the **foreman-rake audits:anonymize** command anonymizes audit records that are older than 90 days. You can specify the number of days to keep the audit records by adding the **days** option and add the number of days.

For example, if you want to anonymize audit records that are older than seven days, enter the following command:

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

11.3. CLEANING UNUSED TASKS

Cleaning unused tasks reduces disk space in the database and limits the rate of disk growth. When you perform regular cleaning, Satellite backup completes faster and overall performance is higher.

To clean unused tasks

The installer has a feature to enable a cron job to automatically remove old tasks. This feature is not enabled by default to avoid unwanted tasks cleanup.

1. Enable the cron job:

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

2. By default, the cron job is scheduled to run every day at 19:45. To adjust to the time, change the value of the **--foreman-plugin-tasks-cron-line** parameter:

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

The previous command schedules the cron job to run every day at 15:00, see **man 5 crontab** for more details on cron format.

To change the period after which to delete all the tasks and to configure further advanced settings of the cron job, change the content of the **/etc/foreman/plugins/foreman-tasks.yaml file**.

11.4. RECOVERING FROM A FULL DISK

The following procedure describes how to resolve the situation when a logical volume (LV) with the Pulp database on it has no free space.

To recover from a full disk

1. Let running Pulp tasks finish but do not trigger any new ones as they can fail due to the full disk.

2. Ensure that the LV with the **/var/lib/pulp** directory on it has sufficient free space. Here are some ways to achieve that:

   a. Remove orphaned content:

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

   This is run weekly so it will not free much space.

   b. Change the download policy from **Immediate** to **On Demand** for as many repositories as possible and remove already downloaded packages. See the Red Hat Knowledgebase solution How to change syncing policy for Repositories on Satellite 6.2 from "Immediate" to "On-Demand" on the Red Hat Customer Portal for instructions.

   c. Grow the file system on the LV with the **/var/lib/pulp** directory on it. For more information, see Growing a File System on a Logical Volume in the *Red Hat Enterprise Linux 7 Logical Volume Manager Administration Guide*.

   NOTE

   If you use an untypical file system (other than for example ext3, ext4, or xfs), you might need to unmount the file system so that it is not in use. In that case:

   - Stop Satellite services:

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

   - Grow the file system on the LV.

   - Start Satellite services:

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

3. If some Pulp tasks failed due to the full disk, run them again.

11.5. RECLAIMING DISK SPACE FROM MONGODB

The MongoDB database can use a large amount of disk space especially in heavily loaded deployments. The following procedure describes how to reclaim some of this disk space.

Prerequisites

- A backup of the MongoDB database. For instructions on creating a backup, see Section 8.1.3, "Performing a Backup without Pulp Content".
- Pulp services are stopped:

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

To reclaim disk space from MongoDB

1. Access the MongoDB shell:

   ```
   # mongo pulp_database
   ```

2. Check the amount of disk space used by MongoDB before a repair:

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

3. Ensure that you have free disk space equal to the size of your current MongoDB database plus 2 GB. If the volume containing the MongoDB database lacks sufficient space, you can mount a separate volume and use that for the repair.
4. Enter the repair command:

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

   Note that the repair command blocks all other operations and can take a long time to complete, depending on the size of the database.

5. Check the amount of disk space used by MongoDB after a repair:

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

6. Start Pulp services:

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

11.6. USING RED HAT INSIGHTS WITH SATELLITE SERVER

You can use Red Hat Insights to diagnose systems and downtime related to security exploits, performance degradation and stability failures. You can use the dashboard to quickly identify key risks to stability, security, or performance. You can sort by category, view details of the impact and resolution, and then determine what systems are affected.

Note that you do not need to add a Red Hat Insights entitlement to your subscription manifest.

To use Red Hat Insights in Satellite, you must first install and register your hosts with Red Hat Insights.

To install or register your host using Puppet, or manually, see Red Hat Insights Getting Started.

Deploying Red Hat Insights Using the Ansible role

You can automate the installation and registration of hosts with Red Hat Insights using the **RedHatInsights.insights-client** Ansible role. To add this role to your Satellite, follow the procedures Chapter 4, *Managing Ansible Roles*.

1. Add the **RedHatInsights.insights-client** role to the hosts. For new hosts, see Creating a Host, or to add the role to an existing host, see Assigning Ansible Roles to Existing Hosts .

2. To run the **RedHatInsights.insights-client** role on your host, navigate to **Hosts** > **All Hosts** and click the name of the host that you want to use.

3. Click the **Run Ansible roles** button.

When the role completes, you can view and work with the host that you add on the **Insights** > **Overview** page of the Satellite web UI.

Additional information

- To apply any system updates to the Red Hat Insights plugin, use **httpd restart** after updating.

- To view the logs for Red Hat Insights and all plugins, go to **/var/log/foreman/production.log**.

- If you have problems connecting to Red Hat Insights, ensure that your certificates are up-to-date. Refresh your subscription manifest to update your certificates.

CHAPTER 12. LOGGING AND REPORTING PROBLEMS

This chapter provides information on how to log and report problems in Red Hat Satellite Server, including information on relevant log files, how to enable debug logging, how to open a support case and attach the relevant log tar files, and how to access support cases within the Satellite web UI.

You can use the log files and other information described in this chapter to do your own troubleshooting, or you can capture these and many more files, as well as diagnostic and configuration information, to send to Red Hat Support if you need further assistance.

12.1. DEBUG LOGGING

Debug logging provides the most detailed log information and can help with troubleshooting issues that can arise with Satellite 6.4 and its components. It is also possible to enable or disable individual loggers for selective logging.

12.1.1. Enabling Debug Logging

In the Satellite CLI, enable debug logging to log detailed debugging information for Satellite 6.4.

Procedure

1. Edit the **/etc/foreman/settings.yaml** file.

    a. Change the logging level to "debug":

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

    b. Select individual logging types:

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

    For more information about loggers, see Section 12.1.2, “List of Loggers and Default Values” .

2. Restart Satellite services:

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

12.1.2. List of Loggers and Default Values

The complete list of loggers with their default values

```
:app:
    :enabled: true
:ldap:
    :enabled: false
```

```
:permissions:
  :enabled: false
:sql:
  :enabled: false
```

12.1.3. Log Files Provided by Satellite

Red Hat Satellite provides system information in the form of notifications and log files.

Table 12.1. Log Files for Reporting and Troubleshooting

Log File	Description of Log File Content
/var/log/candlepin	Subscription management
/var/log/foreman	Foreman
/var/log/foreman-proxy	Foreman proxy
/var/log/httpd	Apache HTTP server
/var/log/foreman-installer/satellite	Satellite installer
/var/log/foreman-installer/capsule	Capsule Server installer
/var/log/libvirt	Virtualization API
/var/log/mongodb	Satellite database
/var/log/pulp	Celerybeat and Celery startup request messages. After startup is complete, messages are logged to **/var/log/messages**.
/var/log/puppet	Configuration management
/var/log/rhsm	Subscription management
/var/log/tomcat6 and **/var/log/tomcat**	Apache web server messages for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7, respectively.
/var/log/messages	Various other log messages related to pulp, rhsm, and goferd.

You can also use the **foreman-tail** command to follow many of the log files related to Satellite. You can run **foreman-tail -l** to list the processes and services that it follows.

On Red Hat Enterprise Linux 7, you can use the journal for more extensive logging information. For more information, see Using the Journal in the *Red Hat Enterprise Linux 7 System Administrator's guide*.

12.1.4. Utilities for Collecting Log Information

There are two utilities available to collect information from log files.

Table 12.2. Log Collecting Utilities

Command	Description
foreman-debug	The **foreman-debug** command collects configuration and log file data for Red Hat Satellite, its back-end services, and system information. This information is collected and written to a tar file. By default, the output tar file is located at /**tmp**/***foreman-debug-xxx.tar.xz***. Additionally, the **foreman-debug** command exports tasks run during the last 60 days. By default, the output tar file is located at /**tmp**/***task-export-xxx.tar.xz***. If the file is missing, see the file /**tmp**/**task-export.log** to learn why task export was unsuccessful. For more information, run **foreman-debug --help**. There is no timeout when running this command.
sosreport	The **sosreport** command is a tool that collects configuration and diagnostic information from a Red Hat Enterprise Linux system, such as the running kernel version, loaded modules, and system and service configuration files. The command also runs external programs (for example: **foreman-debug -g**) to collect Satellite-specific information, and stores this output in a tar file. By default, the output tar file is located at /**var**/**tmp**/***sosreport-XXX-20171002230919.tar.xz***. For more information, run**sosreport --help** or see *What is a sosreport and how can I create one?*. The **sosreport** command calls the**foreman-debug -g** and times out after 500 seconds. If your Satellite Server has large log files or many Satellite tasks, support engineers may require the output of **sosreport** and **foreman-debug** when you open a support case.

IMPORTANT

Both **foreman-debug** and **sosreport** remove security information such as passwords, tokens, and keys while collecting information. However, the tar files can still contain sensitive information about the Red Hat Satellite Server. Red Hat recommends that you send this information directly to the intended recipient and not to a public target.

12.2. RED HAT ACCESS PLUGIN

The Red Hat Access plugin enables you to access several Red Hat Customer Portal services from within the Satellite web UI. The plugin comes preinstalled with Satellite.

The Red Hat Access plug-in provides the following services:

- **Search:** Search solutions in the Customer Portal from within the Satellite web UI.

- **Logs:** Send specific parts (snippets) of the log files to assist in problem-solving. Send these log snippets to the Red Hat Customer Portal diagnostic toolchain.

- **Support:** Access your open support cases, modify an open support case and open a new support case from within the Satellite web UI.

NOTE

To access Red Hat Customer Portal resources, you must log in with your Red Hat Customer Portal user identification and password.

12.2.1. Searching for Solutions

In the Satellite UI, search for solutions with the Red Hat access plugin.

Procedure

1. In the upper right, click **Red Hat Access** > **Search**.
2. If necessary, log in to the Red Hat Customer Portal. In the main panel on the upper right, click Log In.
3. In the **Red Hat Search** field, enter your search query. Search results display in the left-hand **Recommendations** list.
4. In the **Recommendations** list, click a solution. The solution article displays in the main panel.

12.2.2. Searching for Solutions Using Logs

The log file viewer lets you view the log files and isolate log snippets. You can also send the log snippets through the Customer Portal diagnostic tool chain to assist with problem-solving.

In the Satellite UI, find solutions using the log files with the Red Hat Access Plugin.

Procedure

1. In the upper right, click **Red Hat Access** > **Logs**.
2. If necessary, log in to the Red Hat Customer Portal. In the main panel on the upper right, click **Log In**.
3. In the left file tree, select a log file and click the file name.
4. Click **Select File**. A pop-up window displays the log file contents.
5. In the log file, highlight any text sections you want to be diagnosed. The **Red Hat Diagnose** button displays.
6. Click **Red Hat Diagnose**. The system sends the highlighted information to the Red Hat Customer Portal, and provides solutions that closely match the provided log information.
7. If the solution does not match the problem, click **Open a New Support Case**. The support case is populated with the highlighted text from the log file. See Section 12.2.1, “Searching for Solutions”.

12.2.3. Creating Support Cases

In the Satellite UI, create a support case with the Red Hat Access Plugin.

Procedure

1. In the upper right, click **Red Hat Access** > **Support** > **New Case**.
2. If necessary, log in to the Red Hat Customer Portal. In the main panel on the upper right, click Log In.
3. The **Product** and **Product Version** fields are automatically populated. Complete the other relevant fields, as follows:
    - **Summary** – Provide a brief summary of the issue.
    - **Description** – Write a detailed description of the issue.
      Based on the summary provided, recommendations for possible solutions display in the main panel.
4. Click **Next**.
5. Choose the appropriate options, as follows:
    - **Severity** – Select the ticket urgency as 4 (low), 3 (normal), 2 (high), or 1 (urgent).
    - **Case Group** – Based on who needs to be notified, create case groups associated with the support case. Select Case Groups in Red Hat Satellite. Create Case Groups within the Customer Portal.
6. Attach the output of **sosreport** and any required files. Add a file description and click **Attach**.

    NOTE

    - If you have large log files or many Satellite tasks, it is recommended to also attach the output of **foreman-debug**.
    - File names must be less than 80 characters and the maximum file size for attachments uploaded using the web UI is 250 MB. Use FTP for larger files.

7. Click **Submit**. The system uploads the case to the Customer Portal, and provides a case number for your reference.

For additional information, examples, and video tutorials, see the *Red Hat Access: Red Hat Support Tool* knowledgebase article.

12.2.4. Viewing Support Cases

In the Satellite UI, view support cases with the Red Hat Access Plugin.

Procedure

1. In the upper right, click **Red Hat Access** > **Support** > **My Cases**.
2. If necessary, log in to the Red Hat Customer Portal. In the main panel on the upper right, click **Log In**.
3. To search for a specific support case from existing cases, do any of the following:
    - In the **Search** field, provide a keyword or phrase.

- From the drop-down list, choose a specific **Case Group**. Your organization has defined **Case Groups** inside the Red Hat Customer Portal.
- Choose a Case Status.

4. From the results, choose a specific support case and click the **Case ID**. The support case is ready to view.

12.2.5. Updating Support Cases

In the Satellite UI, update your support cases with the Red Hat Access Plugin.

Procedure

1. Complete the instructions from Section 12.2.4, "Viewing Support Cases"
2. In the support case, scroll down to the marked sections to do the following:
   - **Attachments:** - Attach a local file from the system. Add a file name to make it easier to identify.

     NOTE

     File names must be less than 80 characters and the maximum file size for attachments uploaded using the web UI is 250 MB. Use FTP for larger files.

   - **Case Discussion:** - Add any updated information about the case you wish to discuss with Global Support Services. After adding information, click **Add Comment**.

CHAPTER 13. CONFIGURING EXTERNAL AUTHENTICATION

By using external authentication you can derive user and user group permissions from user group membership in an external identity provider. When you use external authentication, you do not have to create these users and maintain their group membership manually on Satellite Server.

Important User and Group Account Information

All user and group accounts must be local accounts. This is to ensure that there are no authentication conflicts between local accounts on your Satellite Server and accounts in your Active Directory domain.

Your system is not affected by this conflict if your user and group accounts exist in both **/etc/passwd** and **/etc/group** files. For example, to check if entries for **puppet**, **apache**, **foreman** and **foreman-proxy** groups exist in both **/etc/passwd** and **/etc/group** files, enter the following commands:

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

Scenarios for Configuring External Authentication

Red Hat Satellite supports the following general scenarios for configuring external authentication:

- Using *Lightweight Directory Access Protocol* (LDAP) server as an external identity provider. LDAP is a set of open protocols used to access centrally stored information over a network. With Satellite, you can manage LDAP entirely through the Satellite web UI. For more information, see Section 13.1, “Using LDAP”. Though you can use LDAP to connect to an IdM or AD server, the setup does not support server discovery, cross-forest trusts, or single sign-on with Kerberos in Satellite’s web UI.

- Using *Red Hat Enterprise Linux Identity Management* (IdM) server as an external identity provider. IdM deals with the management of individual identities, their credentials and privileges used in a networking environment. Configuration using IdM cannot be completed using only the Satellite web UI and requires some interaction with the CLI. For more information see Section 13.2, “Using Identity Management”.

- Using *Active Directory* (AD) integrated with IdM through cross-forest Kerberos trust as an external identity provider. For more information see Section 13.3.5, “Active Directory with Cross-Forest Trust”.

As well as providing access to Satellite Server, hosts provisioned with Satellite can also be integrated with IdM realms. Red Hat Satellite has a realm feature that automatically manages the life cycle of any system registered to a realm or domain provider. For more information, see Section 13.7, “External Authentication for Provisioned Hosts”.

Table 13.1. Authentication Overview

Type	Authentication	User Groups
IdM	Kerberos or LDAP	Yes
Active Directory	Kerberos or LDAP	Yes
POSIX	LDAP	Yes

13.1. USING LDAP

If you require Red Hat Satellite to use **TLS** to establish a secure LDAP connection (LDAPS), first obtain certificates used by the LDAP server you are connecting to and mark them as trusted on the base operating system of your Satellite Server as described below. If your LDAP server uses a certificate chain with intermediate certificate authorities, all of the root and intermediate certificates in the chain must be trusted, so ensure all certificates are obtained. If you do not require secure LDAP at this time, proceed to Section 13.1.2, "Configuring Red Hat Satellite to use LDAP" .

Using SSSD Configuration

Though direct LDAP integration is covered in this section, Red Hat recommends that you use SSSD and configure it against IdM, AD, or an LDAP server. SSSD improves the consistency of the authentication process. For more information about the preferred configurations, see Section 13.3, "Using Active Directory". You can also cache the SSSD credentials and use them for LDAP authentication. For more information on SSSD, see Configuring SSSD in the *Red Hat Enterprise Linux 7 System-Level Authentication Guide*.

13.1.1. Configuring TLS for Secure LDAP

Use the Satellite CLI to configure TLS for secure LDAP (LDAPS).

Procedure

1. Obtain the Certificate from the LDAP Server.

   a. If you use Active Directory Certificate Services, export the Enterprise PKI CA Certificate using the Base-64 encoded X.509 format. See How to configure Active Directory authentication with **TLS** on Satellite 6 for information on creating and exporting a CA certificate from an Active Directory server.

   b. Download the LDAP server certificate to a temporary location on the Red Hat Enterprise Linux system where the Satellite Server is installed and remove it when finished. For example, **/tmp/example.crt**. The filename extensions **.cer** and **.crt** are only conventions and can refer to DER binary or PEM ASCII format certificates.

2. Trust the Certificate from the LDAP Server.
   Red Hat Satellite Server requires the CA certificates for LDAP authentication to be individual files in **/etc/pki/tls/certs/** directory.

   a. Use the **install** command to install the imported certificate into the **/etc/pki/tls/certs/** directory with the correct permissions:

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

   b. Enter the following command as **root** to trust the *example.crt* certificate obtained from the LDAP server:

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

   c. Restart the **httpd** service:

   ```
   # systemctl restart httpd
   ```

13.1.2. Configuring Red Hat Satellite to use LDAP

In the Satellite web UI, configure Satellite to use LDAP.

Note that if you need single sign-on functionality with Kerberos on Satellite's web UI, you should use IdM and AD external authentication instead. See Using Identity Management or Using Active Directory for more information on those options.

Procedure

1. Set the Network Information System (NIS) service boolean to true to prevent SELinux from stopping outgoing LDAP connections:

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

2. Navigate to **Administer** > **LDAP Authentication**.

3. Click **Create Authentication Source**.

4. On the **LDAP server** tab, enter the LDAP server's name, host name, port, and server type. The default port is 389, the default server type is POSIX (alternatively you can select FreeIPA or Active Directory depending on the type of authentication server). For **TLS** encrypted connections, select the **LDAPS** check box to enable encryption. The port should change to 636, which is the default for LDAPS.

5. On the **Account** tab, enter the account information and domain name details. See Section 13.1.3, "Description of LDAP Settings" for descriptions and examples.

6. On the **Attribute mappings** tab, map LDAP attributes to Satellite attributes. You can map login name, first name, last name, email address, and photo attributes. See Section 13.1.4, "Example Settings for LDAP Connections" for examples.

7. On the **Locations** tab, select locations from the left table. Selected locations are assigned to users created from the LDAP authentication source, and available after their first login.

8. On the **Organizations** tab, select organizations from the left table. Selected organizations are assigned to users created from the LDAP authentication source, and available after their first login.

9. Click **Submit**.

10. Configure new accounts for LDAP users:

    - If you did not select **Onthefly Register** check box, see Section 5.1.1, "Creating a User" to create user accounts manually.

    - If you selected the **Onthefly Register** check box, LDAP users can now log in to Satellite using their LDAP accounts and passwords. After they log in for the first time, the Satellite administrator has to assign roles to them manually. See Section 5.1.2, "Assigning Roles to a User" to assign user accounts appropriate roles in Satellite.

13.1.3. Description of LDAP Settings

The following table provides a description for each setting in the **Account** tab.

Table 13.2. Account Tab Settings

Setting	Description
Account	The user name of the LDAP account that has read access to the LDAP server. User name is not required if the server allows anonymous reading, otherwise use the full path to the user's object. For example: `uid=$login,cn=users,cn=accounts,dc=example,dc=com` The **$login** variable stores the username entered on the login page as a literal string. The value is accessed when the variable is expanded. The variable cannot be used with external user groups from an LDAP source because Satellite needs to retrieve the group list without the user logging in. Use either an anonymous, or dedicated service user.
Account password	The LDAP password for the user defined in the **Account username** field. This field can remain blank if the **Account username** is using the **$login** variable.
Base DN	The top level domain name of the LDAP directory.
Groups base DN	The top level domain name of the LDAP directory tree that contains groups.
LDAP filter	A filter to restrict LDAP queries.
Onthefly Register	If this check box is selected, Satellite creates user accounts for LDAP users when they log in to Satellite for the first time. After they log in for the first time, the Satellite administrator has to assign roles to them manually. See Section 5.1.2, "Assigning Roles to a User" to assign user accounts appropriate roles in Satellite.
Usergroup Sync	If this option is selected, the user group membership of a user is automatically synchronized when the user logs in, which ensures the membership is always up to date. If this option is cleared, Satellite relies on a cron job to regularly synchronize group membership (every 30 minutes by default). See To Configure an External User Group: for further context.

13.1.4. Example Settings for LDAP Connections

The following table shows example settings for different types of LDAP connections. The example below uses a dedicated service account called *redhat* that has bind, read, and search permissions on the user and group entries. Note that LDAP attribute names are case sensitive.

Table 13.3. Example Settings for Active Directory, Free IPA or Red Hat Identity Management and POSIX LDAP Connections

Setting	Active Directory	FreeIPA or Red Hat Identity Management	POSIX (OpenLDAP)
Account	DOMAIN\redhat	uid=redhat,cn=users, cn=accounts,dc=example, dc=com	uid=redhat,ou=users, dc=example,dc=com

Setting	Active Directory	FreeIPA or Red Hat Identity Management	POSIX (OpenLDAP)
Account password	P@ssword	-	-
Base DN	DC=example,DC=COM	dc=example,dc=com	dc=example,dc=com
Groups Base DN	CN=Users,DC=example,DC=com	cn=groups,cn=accounts,dc=example,dc=com	cn=employee,ou=userclass,dc=example,dc=com
Login name attribute	userPrincipalName	uid	uid
First name attribute	givenName	givenName	givenName
Last name attribute	sn	sn	sn
Email address attribute	mail	mail	mail

NOTE

userPrincipalName allows the use of whitespace in usernames. The login name attribute **sAMAccountName** (which is not listed in the table above) provides backwards compatibility with legacy Microsoft systems. **sAMAccountName** does not allow the use of whitespace in usernames.

13.1.5. Example LDAP Filters

As an administrator, you can create LDAP filters to restrict the access of specific users to Satellite.

Table 13.4. Example filters for allowing specific users to login

User	Filter
User1, User3	(memberOf=cn=Group1,cn=Users,dc=domain,dc=example)
User2, User3	(memberOf=cn=Group2,cn=Users,dc=domain,dc=example)
User1, User2, User3	(|(memberOf=cn=Group1,cn=Users,dc=domain,dc=example)(memberOf=cn=Group2,cn=Users,dc=domain,dc=example))

LDAP directory structure

The LDAP directory structure that the filters in the example use:

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

LDAP group membership

The group membership that the filters in the example use:

Group	Members
Group1	User1, User3
Group2	User2, User3

13.2. USING IDENTITY MANAGEMENT

This section shows how to integrate Red Hat Satellite Server with an IdM server and how to enable host-based access control.

> **NOTE**
>
> You can attach Identity Management as an external authentication source with no single sign-on support. For more information, see Section 13.1, “Using LDAP”.

Prerequisites

- The Satellite Server has to run on Red Hat Enterprise Linux 7.1 or Red Hat Enterprise Linux 6.6 or later.
- The base operating system of the Satellite Server must be enrolled in the IdM domain by the IdM administrator of your organization.

The examples in this chapter assume separation between IdM and Satellite configuration. However, if you have administrator privileges for both servers, you can configure IdM as described in Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy Guide

13.2.1. Configuring IdM Authentication on Satellite Server

In the Satellite CLI, configure IdM authentication by first creating a host entry on the IdM server.

Procedure

1. On the IdM server, to authenticate, enter the following command and enter your password when prompted:

   ```
   # kinit admin
   ```

2. To verify that you have authenticated, enter the following command:

   ```
   # klist
   ```

3. On the IdM server, create a host entry for the Satellite Server and generate a one-time password, for example:

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

   NOTE

   The generated one-time password must be used on the client to complete IdM-enrollment.

   For more information on host configuration properties, see About Host Entry Configuration Properties in the *Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy* guide.

4. Create an HTTP service for Satellite Server, for example:

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

   For more information on managing services, see Managing Services in the *Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy* guide.

5. On Satellite Server, install the IPA client:

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

6. On Satellite Server, enter the following command as root to configure IdM-enrollment:

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

   Replace *OTP* with the one-time password provided by the IdM administrator.

7. If Satellite Server is running on Red Hat Enterprise Linux 7, enter the following command:

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

   The installer is dependent on packages which, on Red Hat Enterprise Linux 7, are in the optional repository **rhel-7-server-optional-rpms**. On Red Hat Enterprise Linux 6 all necessary packages are in the **base** repository.

8. Set **foreman-ipa-authentication** to true, using the following command:

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

9. Restart Satellite services:

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

External users can now log in to Satellite using their IdM credentials. They can now choose to either log in to Satellite Server directly using their username and password or take advantage of the configured

Kerberos single sign-on and obtain a ticket on their client machine and be logged in automatically. The two-factor authentication with one-time password (2FA OTP) is also supported. If the user in IdM is configured for 2FA, and Satellite Server is running on Red Hat Enterprise Linux 7, this user can also authenticate to Satellite with an OTP.

13.2.2. Configuring Host-Based Authentication Control

HBAC rules define which machine within the domain an IdM user is allowed to access. You can configure HBAC on the IdM server to prevent selected users from accessing the Satellite Server. With this approach, you can prevent Satellite from creating database entries for users that are not allowed to log in. For more information on HBAC, see Configuring Host-Based Access Control in the *Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy* guide.

On the IdM server, configure Host-Based Authentication Control (HBAC).

Procedure

1. On the IdM server, to authenticate, enter the following command and enter your password when prompted:

   ```
   # kinit admin
   ```

2. To verify that you have authenticated, enter the following command:

   ```
   # klist
   ```

3. Create HBAC service and rule on the IdM server and link them together. The following examples use the PAM service name *satellite-prod*. Execute the following commands on the IdM server:

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

4. Add the user who is to have access to the service satellite-prod, and the hostname of the Satellite Server:

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

   Alternatively, host groups and user groups can be added to the *allow_satellite_prod* rule.

5. To check the status of the rule, execute:

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

6. Ensure the allow_all rule is disabled on the IdM server. For instructions on how to do so without disrupting other services see the How to configure HBAC rules in IdM article on the Red Hat Customer Portal.

7. Configure the IdM integration with the Satellite Server as described in Section 13.2.1, "Configuring IdM Authentication on Satellite Server". On the Satellite Server, define the PAM service as root:

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

13.3. USING ACTIVE DIRECTORY

This section shows how to use direct Active Directory (AD) as an external authentication source for Satellite Server.

NOTE

You can attach Active Directory as an external authentication source with no single sign-on support. For more information, see Section 13.1, "Using LDAP".
For an example configuration, see How to configure Active Directory authentication with TLS on Satellite 6.

Direct AD integration means that Satellite Server is joined directly to the AD domain where the identity is stored. The recommended setup consists of two steps:

- Enrolling Satellite Server with the Active Directory server as described in Section 13.3.2, "Enrolling Satellite Server with the AD Server"
- Configuring direct Active Directory integration with GSS-proxy as described in Section 13.3.3, "Configuring Direct AD Integration with GSS-proxy".

13.3.1. GSS-Proxy

The traditional process of Kerberos authentication in Apache requires the Apache process to have read access to the keytab file. GSS-Proxy allows you to implement stricter privilege separation for the Apache server by removing access to the keytab file while preserving Kerberos authentication functionality. When using AD as an external authentication source for Satellite, it is recommended to implement GSS-proxy, because the keys in the keytab file are the same as the host keys.

NOTE

The AD integration requires Red Hat Satellite Server to be deployed on Red Hat Enterprise Linux 7.1 or later.

Perform the following procedures on Red Hat Enterprise Linux that acts as a base operating system for your Satellite Server. For the examples in this section *EXAMPLE.ORG* is the Kerberos realm for the AD domain. By completing the procedures, users that belong to the EXAMPLE.ORG realm can log in to the Satellite Server.

13.3.2. Enrolling Satellite Server with the AD Server

In the Satellite CLI, enroll Satellite Server with the Active Directory server.

Prerequisites

- GSS-proxy and nfs-utils are installed.
  Installing GSS-proxy and nfs-utils:

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

Procedure

1. Install the required packages:

   ```
   # yum install sssd adcli realmd ipa-python-compat krb5-workstation samba-common-tools
   ```

2. Enroll Satellite Server with the AD server. You may need to have administrator permissions to perform the following command:

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

13.3.3. Configuring Direct AD Integration with GSS-proxy

In the Satellite CLI, configure the direct Active Directory integration with GSS-proxy.

Prerequisite

- Satellite is enrolled with the Active Directory server.
  For more information, see Section 13.3.2, "Enrolling Satellite Server with the AD Server" .

Procedure

1. Create the **/etc/ipa/** directory and the **default.conf** file:

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

2. To the **default.conf** file, add the following content:

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

3. Create the **/etc/net-keytab.conf** file with the following content:

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

4. Determine the effective user ID of the Apache user:

   ```
   # id apache
   ```

   Apache user must not have access to the keytab file.

5. Create the **/etc/gssproxy/00-http.conf** file with the following content:

   ```
   [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. Insert the following line at the beginning of the **/etc/krb5.conf** file:

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

7. Create a keytab entry:

   ```
   # 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. Enable IPA authenication in Satellite:

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

9. Start and enable the **gssproxy** service:

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

10. Configure the Apache server to use the gssproxy service:

    a. Create the **/etc/systemd/system/httpd.service** file with the following content:

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

    b. Apply changes to the service:

    ```
    # systemctl daemon-reload
    ```

11. Start and enable the **httpd** service:

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

12. Verify that SSO is working as expected.
    With a running Apache server, users making HTTP requests against the server are authenticated if the client has a valid Kerberos ticket.

    a. Retrieve the Kerberos ticket of the LDAP user, using the following command:

    ```
    # kinit ldapuser
    ```

    b. View the Kerberos ticket, using the following command:

    ```
    # klist
    ```

    c. View output from successful SSO-based authentication, using the following command:

```
# 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. Kerberos Configuration in Web Browsers

For information on configuring the Firefox browser see Configuring Firefox to Use Kerberos for Single Sign-On in the *Red Hat Enterprise Linux System-Level Authentication* guide.

If you use the Internet Explorer browser, add Satellite Server to the list of Local Intranet or Trusted sites, and turn on the *Enable Integrated Windows Authentication* setting. See the Internet Explorer documentation for details.

NOTE

With direct AD integration, HBAC through IdM is not available. As an alternative, you can use Group Policy Objects (GPO) that enable administrators to centrally manage policies in AD environments. To ensure correct GPO to PAM service mapping, use the following sssd configuration:

```
access_provider = ad
ad_gpo_access_control = enforcing
ad_gpo_map_service = +foreman
```

Here, *foreman* is the PAM service name. For more information on GPOs, please refer to the Red Hat Enterprise Linux Windows Integration Guide .

13.3.5. Active Directory with Cross-Forest Trust

Kerberos can create **cross-forest trust** that defines a relationship between two otherwise separate domain forests. A domain forest is a hierarchical structure of domains; both AD and IdM constitute a forest. With a trust relationship enabled between AD and IdM, users of AD can access Linux hosts and services using a single set of credentials. For more information on cross-forest trusts, see Creating Cross-forest Trusts with Active Directory and Identity Management in the *Red Hat Enterprise Linux Windows Integration* guide.

From the Satellite point of view, the configuration process is the same as integration with IdM server without cross-forest trust configured. The Satellite Server has to be enrolled in the IPM domain and integrated as described in Section 13.2, “Using Identity Management” .

13.3.6. Configuring the IdM Server to Use Cross-Forest Trust

On the IdM server, configure the server to use **cross-forest trust**.

Procedure

1. Enable HBAC:

    a. Create an external group and add the AD group to it.

    b. Add the new external group to a POSIX group.

    c. Use the POSIX group in a HBAC rule.

2. Configure sssd to transfer additional attributes of AD users.
   - Add the AD user attributes to the *nss* and *domain* sections in **/etc/sssd/sssd.conf**. For example:

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

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

13.4. CONFIGURING EXTERNAL USER GROUPS

Satellite does not associate external users with their user group automatically. You must create a user group with the same name as in the external source on Satellite. Members of the external user group then automatically become members of the Satellite user group and receive the associated permissions.

The configuration of external user groups depends on the type of external authentication.

To assign additional permissions to an external user, add this user to an internal user group that has no external mapping specified. Then assign the required roles to this group.

Prerequisites

- If you use an LDAP server, configure Satellite to use LDAP authentication. For more information see Section 13.1, "Using LDAP".
  When using external user groups from an LDAP source, you cannot use the **$login** variable as a substitute for the account user name. You must use either an anonymous or dedicated service user.
- If you use an IdM or AD server, configure Satellite to use IdM or AD authentication. For more information, see Chapter 13, *Configuring External Authentication*.
- Ensure that at least one external user authenticates for the first time.
- Retain a copy of the external group names you want to use. To find the group membership of external users, enter the following command:

  ```
  # id username
  ```

To Configure an External User Group:

1. In the Satellite web UI, navigate to **Administer** > **User Groups**, and click **Create User Group**.
2. Specify the name of the new user group. Do not select any users as they would be added automatically when refreshing the external user group.
3. Click the **Roles** tab and select the roles you want to assign to the user group. Alternatively, select the **Administrator** check box to assign all available permissions.
4. Navigate to **External groups** > **Add external user group** and select an authentication source from the **Auth source** drop-down menu.
   Specify the exact name of the external group in the **Name** field.
5. Click **Submit**.

13.5. REFRESHING EXTERNAL USER GROUPS FOR LDAP

To set the LDAP source to synchronize user group membership automatically on user login, in the **Auth Source** page, select the **Usergroup Sync** option. If this option is not selected, LDAP user groups are refreshed automatically through a scheduled cron job synchronizing the LDAP Authentication source every 30 minutes by default.

If the user groups in the LDAP Authentication source change in the lapse of time between scheduled tasks, the user can be assigned to incorrect external user groups. This is corrected automatically when the scheduled task runs.

Use this procedure to refresh the LDAP source manually.

Procedure

1. Navigate to **Administer** > **Usergroups** and select a user group.
2. Navigate to the **External Groups** tab and click **Refresh** to the right of the required user group.

For CLI Users

Enter the following command:

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

13.6. REFRESHING EXTERNAL USER GROUPS FOR IDM OR AD

External user groups based on IdM or AD are refreshed only when a group member logs in to Satellite. It is not possible to alter user membership of external user groups in the Satellite web UI, such changes are overwritten on the next group refresh.

13.7. EXTERNAL AUTHENTICATION FOR PROVISIONED HOSTS

Use this section to configure Satellite Server or Capsule Server for IdM realm support, then add hosts to the IdM realm group.

Prerequisites

You require the following setup to configure external authentication for provisioned hosts:

- Satellite Server that is registered to the Content Delivery Network or an external Capsule Server that is registered to Satellite Server.
- A deployed realm or domain provider such as Red Hat Identity Management.

To install and configure IdM packages on Red Hat Satellite Server or Red Hat Satellite Capsule Server:

To use IdM for provisioned hosts, complete the following steps to install and configure IdM packages on Red Hat Satellite Server or Red Hat Satellite Capsule Server:

1. Install the **ipa-client** package:

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

2. Configure the server as an IdM client:

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

3. Create a realm proxy user, **realm-capsule**, and the relevant roles in Red Hat Identity Management:

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

   Note the principal name that returns and your Identity Management server configuration details because you require them for the following procedure.

To configure Satellite Server or Capsule Server for IdM Realm Support:

Complete the following procedure on Satellite and every Capsule that you want to use:

1. Copy the **/root/freeipa.keytab** file to any Capsule Server that you want to include in the same principal and realm:

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

2. Move the **/root/freeipa.keytab** file to the **/etc/foreman-proxy** directory and set the ownership settings to the **foreman-proxy** user:

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

3. Enter the following command on all Capsules that you want to include in the realm. If you use the integrated Capsule on Satellite, enter this command on Satellite Server:

   ```
   # 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
   ```

   You can also use these options when you first configure the Red Hat Satellite Server.

4. Ensure that the most updated versions of the ca-certificates package is installed and trust the IdM Certificate Authority:

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

5. Optional: If you configure IdM on an existing Satellite Server or Capsule Server, complete the following steps to ensure that the configuration changes take effect:

   a. Restart the **foreman-proxy** service:

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

   b. In the Satellite web UI, navigate to **Infrastructure** > **Capsules**.

c. Locate the Capsule you have configured for IdM and from the list in the **Actions** column, select **Refresh**.

To create a realm for the IdM-enabled Capsule

After you configure your integrated or external Capsule with IdM, you must create a realm and add the IdM-configured Capsule to the realm.

To create a realm, complete the following steps:

1. In the Satellite web UI, navigate to **Infrastructure** > **Realms** and click **Create Realm**.
2. In the **Name** field, enter a name for the realm.
3. From the **Realm Type** list, select the type of realm.
4. From the **Realm Capsule** list, select the Capsule Server where you have configured IdM.
5. Click the **Locations** tab and from the **Locations** list, select the location where you want to add the new realm.
6. Click the **Organizations** tab and from the **Organizations** list, select the organization where you want to add the new realm.
7. Click **Submit**.

Updating Host Groups with Realm Information

You must update any host groups that you want to use with the new realm information.

1. Navigate to **Configure** > **Host Groups**, select the host group that you want to update, and click the **Network** tab.
2. From the **Realm** list, select the realm you create as part of this procedure, and then click **Submit**.

Adding Hosts to an IdM Host Group

Red Hat Enterprise Linux Identity Management (IdM) supports the ability to set up automatic membership rules based on a system’s attributes. Red Hat Satellite’s realm feature provides administrators with the ability to map the Red Hat Satellite host groups to the IdM parameter **userclass** which allow administrators to configure automembership.

When nested host groups are used, they are sent to the IdM server as they are displayed in the Red Hat Satellite User Interface. For example, "Parent/Child/Child".

Satellite Server or Capsule Server sends updates to the IdM server, however automembership rules are only applied at initial registration.

To Add Hosts to an IdM Host Group:

1. On the IdM server, create a host group:

   ```
   # ipa hostgroup-add hostgroup_name --desc=hostgroup_description
   ```

2. Create an **automembership** rule:

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

Where you can use the following options:

- **automember-add** flags the group as an automember group.
- **--type=hostgroup** identifies that the target group is a host group, not a user group.
- ***automember_rule*** adds the name you want to identify the automember rule by.

3. Define an automembership condition based on the **userclass** attribute:

```
# 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
----------------------------
```

Where you can use the following options:

- **automember-add-condition** adds regular expression conditions to identify group members.
- **--key=userclass** specifies the key attribute as **userclass**.
- **--type=hostgroup** identifies that the target group is a host group, not a user group.
- **--inclusive-regex=** *^webserver* identifies matching values with a regular expression pattern.
- *hostgroup_name* - identifies the target host group's name.

When a system is added to Satellite Server's *hostgroup_name* host group, it is added automatically to the Identity Management server's "*hostgroup_name*" host group. IdM host groups allow for Host-Based Access Controls (HBAC), sudo policies and other IdM functions.

CHAPTER 14. EXTENDING SATELLITE SERVER FUNCTIONALITY

Red Hat Satellite Server can be extended by installing plugins. For example, you can extend hosts orchestration with the Foreman Hooks plug-in. For more information about Foreman Hooks, see the Using Foreman Hooks in Satellite Server article on the Red Hat Customer Portal. The plugins are available as RPM packages in the Red Hat repositories and the Foreman repositories.

Plugins for Satellite typically include the word **foreman** in the RPM package name and the plugins for Capsule include the word **smart_proxy** in the name.

The plugins provided by Red Hat can be searched and installed using the **yum** command from the Satellite **CLI**.

The *upstream* Satellite plugins are available in the Foreman repositories. Each release of Foreman has a separate repository containing plugins for that release. For more information about configuring the Foreman repository, see Section 14.3, “Configuring the Foreman Repository”.

IMPORTANT

Red Hat supports the Foreman API but not the plugins installed from the Foreman repository.

14.1. SEARCHING FOR PLUGINS

Search available plugins using the Satellite **CLI**.

NOTE

To search *upstream* plugins as well, configure the Foreman repository as described in Section 14.3, “Configuring the Foreman Repository”

Procedure

- As root user, search for packages with "-foreman" in the package name using **yum search**. Example - Searching rubygem plugin for Satellite:

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

14.2. INSTALLING PLUGINS

Install plugins using the Satellite CLI. Ensure you install plugins compatible with the version of Foreman on your system. You can view an RPM package description to confirm the identity of a plugin using the **yum info** or **rpm -qi** command.

NOTE

To install *upstream* plugins, configure the Foreman repository as described in Section 14.3, "Configuring the Foreman Repository".

Procedure

1. Install the required plugin using **yum install**.
   Example: Installing the *tfm-rubygem-foreman_templates* plugin:

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

2. Restart **foreman-maintain** service.

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

To verify the install, use **yum** to list installed plugins:

- Example: Verifying rubygem-foreman plugin is installed:

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

- You can also list Capsule plugins using **yum**:

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

14.3. CONFIGURING THE FOREMAN REPOSITORY

Configure the Foreman repository using the Satellite CLI to install the *upstream* plugins. After you configure the repository, you can search and install the plugins using the **yum** command from Satellite CLI. The Foreman packages are not currently GPG signed.

For additional information on foreman plugins, see the Popular Plugins and List of Plugins sections on the *Foreman* website.

Procedure

1. Determine the Foreman release with **rpm** command.

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

2. Create an rpm configuration file.

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

3. Add the following content to the file:

```
[foreman-plugins]
name=Foreman plugins
baseurl=http://yum.theforeman.org/plugins/1.20/el7/x86_64/
enabled=1
gpgcheck=0
```

Replace the version number in the URL to the required Foreman release number.

CHAPTER 15. MONITORING RESOURCES

The following chapter details how to configure monitoring and reporting for managed systems. This includes host configuration, content views, compliance, subscriptions, registered hosts, promotions and synchronization.

15.1. USING THE RED HAT SATELLITE CONTENT DASHBOARD

The Red Hat Satellite content dashboard contains various widgets which provide an overview of the host configuration, Content Views, compliance reports, subscriptions and hosts currently registered, promotions and synchronization, and a list of the latest notifications.

Navigate to **Monitor** > **Dashboard** to access the content dashboard. The dashboard can be rearranged by clicking on a widget and dragging it to a different position. The following widgets are available:

Host Configuration Status

An overview of the configuration states and the number of hosts associated with it during the last reporting interval. The following table shows the descriptions of the possible configuration states.

Table 15.1. Host Configuration States

Icon	State	Description
🟦	**Hosts that had performed modifications without error**	Host that successfully performed modifications during the last reporting interval.
🟥	**Hosts in error state**	Hosts on which an error was detected during the last reporting interval.
🟩	**Good host reports in the last 35 minutes**	Hosts without error that did not perform any modifications in the last 35 minutes.
🟪	**Hosts that had pending changes**	Hosts on which some resources would be applied but Puppet was configured to run in the **noop** mode.
🟩	**Out of sync hosts**	Hosts that were not synchronized and the report was not received during the last reporting interval.
🟧	**Hosts with no reports**	Hosts for which no reports were collected during the last reporting interval.
🟦	**Hosts with alerts disabled**	Hosts which are not being monitored.

Click the particular configuration status to view hosts associated with it.

Host Configuration Chart

A pie chart shows the proportion of the configuration status and the percentage of all hosts associated with it.

Latest Events

A list of messages produced by hosts including administration information, product and subscription changes, and any errors.

Monitor this section for global notifications sent to all users and to detect any unusual activity or errors.

Run Distribution (last 30 minutes)

A graph shows the distribution of the running Puppet agents during the last puppet interval which is 30 minutes by default. In this case, each column represents a number of reports received from clients during 3 minutes.

New Hosts

A list of the recently created hosts. Click the host for more details.

Task Status

A summary of all current tasks, grouped by their state and result. Click the number to see the list of corresponding tasks.

Latest Warning/Error Tasks

A list of the latest tasks that have been stopped due to a warning or error. Click a task to see more details.

Discovered Hosts

A list of all bare-metal hosts detected on the provisioning network by the Discovery plug-in.

Latest Errata

A list of all errata available for hosts registered to Satellite.

Content Views

A list of all Content Views in Satellite and their publish status.

Sync Overview

An overview of all products or repositories enabled in Satellite and their synchronization status. All products that are in the queue for synchronization, are unsynchronized or have been previously synchronized are listed in this section.

Host Subscription Status

An overview of the subscriptions currently consumed by the hosts registered to Satellite. A subscription is a purchased certificate that unlocks access to software, upgrades, and security fixes for hosts. The following table shows the possible states of subscriptions.

Table 15.2. Host Subscription States

Icon	State	Description
🟥	**Invalid**	Hosts that have products installed, but are not correctly subscribed. These hosts need attention immediately.

Icon	State	Description
🟧	**Partial**	Hosts that have a subscription and a valid entitlement, but are not using their full entitlements. These hosts should be monitored to ensure they are configured as expected.
🟩	**Valid**	Hosts that have a valid entitlement and are using their full entitlements.

Click the subscription type to view hosts associated with subscriptions of the selected type.

Subscription Status

An overview of the current subscription totals that shows the number of active subscriptions, the number of subscriptions that expire in the next 120 days, and the number of subscriptions that have recently expired.

Host Collections

A list of all host collections in Satellite and their status, including the number of content hosts in each host collection.

Virt-who Configuration Status

An overview of the status of reports received from the **virt-who** daemon running on hosts in the environment. The following table shows the possible states.

Table 15.3. Virt-who Configuration States

State	Description
No Reports	No report has been received because either an error occurred during the virt-who configuration deployment, or the configuration has not been deployed yet, or virt-who cannot connect to Foreman during the scheduled interval.
No Change	No report has been received because hypervisor did not detect any changes on the virtual machines, or virt-who failed to upload the reports during the scheduled interval. If you added a virtual machine but the configuration is in the **No Change** state, check that virt-who is running.
OK	The report has been received without any errors during the scheduled interval.
Total Configurations	A total number of virt-who configurations.

Click the configuration status to see all configurations in this state.

The widget also lists the three latest configurations in the **No Change** state under **Latest Configurations Without Change**.

Latest Compliance Reports

A list of the latest compliance reports. Each compliance report shows a number of rules passed (P), failed (F), or othered (O). Click the host for the detailed compliance report. Click the policy for more details on that policy.

Compliance Reports Breakdown

A pie chart shows the distribution of compliance reports according to their status.

Red Hat Insights Actions

Red Hat Insights is a tool embedded in Satellite that checks the environment and suggests actions you can take. The actions are divided into 4 categories: Availability, Stability, Performance, and Security.

Red Hat Insights Risk Summary

A table shows the distribution of the actions according to the risk levels. Risk level represents how critical the action is and how likely it is to cause an actual issue. The possible risk levels are: Low, Medium, High, and Critical.

NOTE

It is not possible to change the date format displayed in the Satellite web UI.

15.1.1. Managing Tasks

Red Hat Satellite keeps a complete log of all planned or performed tasks, such as repositories synchronised, errata applied, Content Views published, and so on. To review the log, navigate to **Monitor** > **Tasks**. The page enables you to search for specific tasks, view their status and details, and resume those that resulted in an error, if applicable.

The tasks are managed using the Dynflow engine. Remote tasks have a timeout which can be adjusted as needed.

To Adjust Timeout Settings:

1. Navigate to **Administer** > **Settings**.

2. Enter *%_timeout* in the search box and click **Search**. The search should return four settings, including a description.

3. In the **Value** column, click the icon next to a number to edit it.

4. Enter the desired value in seconds, and click **Save**.

NOTE

Adjusting the *%_finish_timeout* values might help in case of low bandwidth. Adjusting the *%_accept_timeout* values might help in case of high latency.

When a task is initialized, any back-end service that will be used in the task, such as Candlepin or Pulp, will be checked for correct functioning. If the check fails, you will receive an error similar to the following one:

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

If the back-end service checking feature turns out to be causing any trouble, it can be disabled as follows.

To Disable Checking for Services:

1. Navigate to **Administer** > **Settings**.
2. Enter *check_services_before_actions* in the search box and click **Search**.
3. In the **Value** column, click the icon to edit the value.
4. From the drop-down menu, select **false**.
5. Click **Save**.

15.2. CONFIGURING RSS NOTIFICATIONS

To view Satellite event notification alerts, click the **Notifications** icon in the upper right of the screen.

By default, the Notifications area displays RSS feed events published in the Red Hat Satellite Blog . The feed is refreshed every 12 hours and the Notifications area is updated whenever new events become available.

You can configure the RSS feed notifications by changing the URL feed. The supported feed format is RSS 2.0 and Atom. For an example of the RSS 2.0 feed structure, see the Red Hat Satellite Blog feed . For an example of the Atom feed structure, see the Foreman blog feed .

To Configure RSS Feed Notifications:

1. Navigate to **Administer** > **Settings** and select the **Notifications** tab.
2. In the RSS URL row, click the edit icon in the **Value** column and type the required URL.
3. In the RSS enable row, click the edit icon in the **Value** column to enable or disable this feature.

15.3. MONITORING SATELLITE SERVER

From the **About** page in the Satellite Server web UI, you can find an overview of the following:

- System Status, including Capsules, Available Providers, Compute Resources, and Plug-ins
- Support information
- System Information
- Backend System Status
- Installed packages

To navigate to the **About** page:

- In the upper right corner of the Satellite Server web UI, click **Administer** > **About**.

NOTE

After Pulp failure, the status of Pulp might show **OK** instead of **Error** for up to 10 minutes due to synchronization delay.

15.4. MONITORING CAPSULE SERVER

The following section shows how to use the Satellite web UI to find Capsule information valuable for maintenance and troubleshooting.

15.4.1. Viewing General Capsule Information

Navigate to **Infrastructure** > **Capsules** to view a table of Capsule Servers registered to the Satellite Server. The information contained in the table answers the following questions:

Is the Capsule Server running?

This is indicated by a green icon in the **Status** column. A red icon indicates an inactive Capsule, use the **service foreman-proxy restart** command on the Capsule Server to activate it.

What services are enabled on the Capsule Server?

In the **Features** column you can verify if the Capsule for example provides a DHCP service or acts as a Pulp node. Capsule features can be enabled during installation or configured in addition. For more information, see Installing Capsule Server.

What organizations and locations is the Capsule Server assigned to?

A Capsule Server can be assigned to multiple organizations and locations, but only Capsules belonging to the currently selected organization are displayed. To list all Capsules, select **Any Organization** from the context menu in the top left corner.
After changing the Capsule configuration, select **Refresh** from the drop-down menu in the **Actions** column to make sure the Capsule table is up to date.

Click the Capsule name to view further details. At the **Overview** tab, you can find the same information as in the Capsule table. In addition, you can answer to the following questions:

Which hosts are managed by the Capsule Server?

The number of associated hosts is displayed next to the **Hosts managed** label. Click the number to view the details of associated hosts.

How much storage space is available on the Capsule Server?

The amount of storage space occupied by the Pulp content in **/var/lib/pulp**, **/var/lib/pulp/content**, and **/var/lib/mongodb** is displayed. Also the remaining storage space available on the Capsule can be ascertained.

15.4.2. Monitoring Services

Navigate to **Infrastructure** > **Capsules** and click the name of the selected Capsule. At the **Services** tab, you can find basic information on Capsule services, such as the list of DNS domains, or the number of Pulp workers. The appearance of the page depends on what services are enabled on the Capsule Server. Services providing more detailed status information can have dedicated tabs at the Capsule page (see Section 15.4.3, “Monitoring Puppet”).

15.4.3. Monitoring Puppet

Navigate to **Infrastructure** > **Capsules** and click the name of the selected Capsule. At the **Puppet** tab you can find the following:

- A summary of Puppet events, an overview of latest Puppet runs, and the synchronization status of associated hosts at the **General** sub-tab.
- A list of Puppet environments at the **Environments** sub-tab.

At the **Puppet CA** tab you can find the following:

- A certificate status overview and the number of autosign entries at the **General** sub-tab.
- A table of CA certificates associated with the Capsule at the **Certificates** sub-tab. Here you can inspect the certificate expiry data, or cancel the certificate by clicking **Revoke**.
- A list of autosign entries at the **Autosign entries** sub-tab. Here you can create an entry by clicking **New** or delete one by clicking **Delete**.

15.5. MONITORING TRENDS

You can use trends to track changes in your infrastructure over time, such as Puppet reports or Facts, and then plan accordingly.

To View a Trend:

1. Navigate to **Monitor** > **Trends**.
2. On the Trends page, select the trend you want to view from the **Trends** list.

To Create a Trend:

1. Navigate to **Monitor** > **Trends**.
2. On the Trends page, click the **Add Trend Counter**.
3. From the **Trend type** list, select the category for the new trend.
4. From the **Trendable** list, select the subject for the new trend (if applicable).
5. In the **Name** field, enter a name for the new trend.
6. Click **Submit**.

NOTE

If this is the first trend, create a **cron** job to collect trend data:

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

You can set the interval for trend data collection. For example, to collect data once an hour, on the hour:

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

CHAPTER 16. SEARCHING AND BOOKMARKING

The Satellite web UI features powerful search functionality which is available on most pages of the web UI. It enables you to search all kinds of resources that Satellite Server manages. Searches accept both free text and syntax-based queries, which can be built using extensive input prediction. Search queries can be saved as bookmarks for future reuse.

16.1. BUILDING SEARCH QUERIES

As you start typing a search query, a list of valid options to complete the current part of the query appears. You can either select an option from the list and keep building the query using the prediction, or continue typing. To learn how free text is interpreted by the search engine, see Section 16.2, “Using Free Text Search”.

16.1.1. Query Syntax

> *parameter operator value*

Available fields, resources to search, and the way the query is interpreted all depend on context, that is, the page where you perform the search. For example, the field "hostgroup" on the Hosts page is equivalent to the field "name" on the Host Groups page. The field type also determines available operators and accepted values. For a list of all operators, see Operators. For descriptions of value formats, see Values.

16.1.2. Operators

All operators that can be used between *parameter* and *value* are listed in the following table. Other symbols and special characters that might appear in a prediction-built query, such as colons, do not have special meaning and are treated as free text.

Table 16.1. Comparison Operators Accepted by Search

Operator	Short Name	Description	Example
=	EQUALS	Accepts numerical, temporal, or text values. For text, exact case sensitive matches are returned.	**hostgroup = RHEL7**
!=	NOT EQUALS		
~	LIKE	Accepts text or temporal values. Returns case insensitive matches. Accepts the following wildcards: _ for a single character, % or * for any number of characters including zero. If no wildcard is specified, the string is treated as if surrounded by wildcards: %rhel7%	**hostgroup ~ rhel%**
!~	NOT LIKE		

Operator	Short Name	Description	Example
>	GREATER THAN	Accepts numerical or temporal values. For temporal values, the operator > is interpreted as "later than", and < as "earlier than". Both operators can be combined with EQUALS: >= <=	**registered_at > 10-January-2017** The search will return hosts that have been registered after the given date, that is, between 10th January 2017 and now. **registered_at <= Yesterday** The search will return hosts that have been registered yesterday or earlier.
<	LESS THAN		
^	IN	Compares an expression against a list of values, as in SQL. Returns matches that contain or not contain the values, respectively.	**release_version !^ 7**
!^	NOT IN		
HAS or set?		Returns values that are present or not present, respectively.	**has hostgroup** or **set? hostgroup** On the Puppet Classes page, the search will return classes that are assigned to at least one host group. **not has hostgroup** or **null? hostgroup** On the Dashboard with an overview of hosts, the search will return all hosts that have no assigned host group.
NOT HAS or null?			

Simple queries that follow the described syntax can be combined into more complex ones using logical operators AND, OR, and NOT. Alternative notations of the operators are also accepted:

Table 16.2. Logical Operators Accepted by Search

Operator	Alternative Notations			Example
and	&	&&	<whitespace>	**class = motd AND environment ~ production**
or	|	||		**errata_status = errata_needed || errata_status = security_needed**
not	–	!		**hostgroup ~ rhel7 not status.failed**

16.1.3. Values

Text Values

Text containing whitespaces must be enclosed in quotes. A whitespace is otherwise interpreted as the AND operator.
Examples:

hostgroup = "Web servers"

The search will return hosts with assigned host group named "Web servers".

hostgroup = Web servers

The search will return hosts in the host group Web with any field matching %servers%.

Temporal Values

Many date and time formats are accepted, including the following:

- "10 January 2017"
- "10 Jan 2017"
- 10-January-2017
- 10/January/2017
- "January 10, 2017"
- Today, Yesterday, and the like.

WARNING

Avoid ambiguous date formats, such as 02/10/2017 or 10-02-2017.

16.2. USING FREE TEXT SEARCH

When you enter free text, it will be searched for across multiple fields. For example, if you type "64", the search will return all hosts that have that number in their name, IP address, MAC address, and architecture.

NOTE

Multi-word queries must be enclosed in quotes, otherwise the whitespace is interpreted as the AND operator.

Because of searching across all fields, free text search results are not very accurate and searching can be slow, especially on a large number of hosts. For this reason, we recommend that you avoid free text and use more specific, syntax-based queries whenever possible.

16.3. MANAGING BOOKMARKS

You can save search queries as bookmarks for reuse. You can also delete or modify a bookmark.

Bookmarks appear only on the page on which they were created. On some pages, there are default bookmarks available for the common searches, for example, all **active** or **disabled** hosts.

16.3.1. Creating Bookmarks

This section details how to save a search query as a bookmark. You must save the search query on the relevant page to create a bookmark for that page, for example, saving a host related search query on the Hosts page.

To Create a Bookmark:

1. Navigate to the page where you want to create a bookmark.
2. In the **Search** field, enter the search query you want to save.
3. Select the arrow to the right of the **Search** button and then select **Bookmark this search**.
4. In the **Name** field, enter a name for the new bookmark.
5. In the **Search query** field, ensure your search query is correct.
6. Ensure the **Public** check box is set correctly:
   - Select the **Public** check box to set the bookmark as public and visible to all users.
   - Clear the **Public** check box to set the bookmark as private and only visible to the user who created it.
7. Click **Submit**.

To confirm the creation, either select the arrow to the right of the **Search** button to display the list of bookmarks, or navigate to **Administer** > **Bookmarks** and then check the **Bookmarks** list for the name of the bookmark.

16.3.2. Deleting Bookmarks

You can delete bookmarks on the Bookmarks page.

To Delete a Bookmark:

1. Navigate to **Administer** > **Bookmarks**.
2. On the Bookmarks page, click **Delete** for the Bookmark you want to delete.
3. When the confirmation window opens, click **OK** to confirm the deletion.

To confirm the deletion, check the **Bookmarks** list for the name of the bookmark.

APPENDIX A. SATELLITE SETTINGS

Red Hat Satellite Server settings can be found on the **Administer** > **Settings** page.

Table A.1. Satellite Settings

Tab	Setting	Default value	Description
Provisioning	Type of name generator	**Random-based**	Specifies the method used to generate a host name when creating a new host. The default **Random-based** option generates a unique random host name which you can but do not have to use. This is useful for users who create many hosts and do not know how to name them. The **MAC-based** option is for bare-metal hosts only. If you delete a host and create it later on, it receives the same host name based on the MAC address. This can be useful for users who recycle servers and want them to always get the same host name. The **Off** option disables the name generator function and leaves the host name field blank.
	Safemode rendering	**Yes**	Enables safe mode rendering of provisioning templates. The default and recommended option **Yes** denies the access to variables and any object that is not whitelisted within Satellite. When set to **No**, any object may be accessed by a user with permission to use templating features, either via editing of templates, parameters or smart variables. This permits users full remote code execution on Satellite Server, effectively disabling all authorization. This is not a safe option, especially in bigger companies.
General	Fix DB cache	**No**	Satellite maintains a cache of permissions and roles. When set to **Yes**, Satellite recreates this cache on the next restart.