Red Hat Satellite 6.10

管理 Red Hat Satellite

管理红帽卫星的指南。

Last Updated: 2024-01-31

Red Hat Satellite 6.10 管理 Red Hat Satellite

管理红帽卫星的指南。

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

法律通告

摘要

本指南提供了有关如何配置和管理 Red Hat Satellite 6 服务器的说明。在继续执行此工作流前，您必须已成功安装 Red Hat Satellite 6 服务器和任何所需的胶囊服务器。

目录

第 1 章 访问 RED HAT SATELLITE

在安装和配置 Red Hat Satellite 后，使用 Web 用户界面登录 Satellite 以进行进一步配置。

1.1. 安装 KATELLO ROOT CA 证书

第一次登录 Satellite 时，您可能会看到一条警告信息，通知您是使用默认自签名证书，且您可能无法在浏览器中安装 root CA 证书前，将这个浏览器连接到 Satellite。使用以下步骤在 Satellite 上找到 root CA 证书，并在浏览器中安装它。

先决条件

您的 Red Hat Satellite 已安装并进行了配置。

流程

1. 识别 Satellite 服务器的完全限定域名：

```
# hostname -f
```

2. 使用 Web 浏览器指向完全限定域名，访问卫星服务器上的 **pub** 目录：

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

3. 当您第一次访问 Satellite 时，Web 浏览器中会显示不受信任的连接警告。接受自签名证书并添加 Satellite URL 作为安全例外，以覆盖设置。根据所使用的浏览器，这个过程可能会有所不同。在您接受安全例外前，请确保 Satellite URL 有效。

4. 选择 **katello-server-ca.crt**。

5. 将证书作为证书颁发机构导入到浏览器中，并信任它来识别网站。

手动导入 Katello Root CA 证书

如果在浏览器中无法添加安全例外，请手动导入 Katello root CA 证书。

1. 在 Satellite CLI 中，将 **katello-server-ca.crt** 文件复制到用于访问 web UI 的机器：

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

2. 在浏览器中，将 **katello-server-ca.crt** 证书导入为证书颁发机构，并信任它来识别网站。

1.2. 登录到 SATELLITE

使用 Web 用户界面登录 Satellite 以进行进一步配置。

先决条件

确保您的浏览器中安装了 Katello root CA 证书。更多信息请参阅 第 1.1 节 “安装 Katello Root CA 证书”。

流程

1. 使用指向完全限定域名的 Web 浏览器访问卫星服务器：

> https://*satellite.example.com*/

2. 输入配置过程中创建的用户名和密码。如果在配置过程中没有创建用户，则默认用户名是 *admin*。如果登录时出现问题，您可以重置密码。更多信息请参阅 第 1.5 节 “重置管理用户密码”。

1.3. 在卫星 WEB UI 中导航标签

使用导航标签页浏览卫星 Web UI。

表 1.1. 导航标签

导航标签	描述
任何上下文	点这个标签页更改机构和位置。如果没有选择组织或位置，则默认组织为 *Any Organization*，默认位置为 *Any Location*。使用此标签页更改为不同的值。
Monitor	提供概述仪表板和报告。
内容	提供内容管理工具。这包括内容视图、激活码和生命周期环境。
主机	提供主机清单和调配配置工具。
配置	提供常规配置工具和数据，包括主机组和 Puppet 数据。
基础架构	提供用于配置 Satellite 6 如何与环境交互的工具。
用户名	为用户提供管理，用户可在其中编辑其个人信息。
	提供事件通知，使管理员能够了解重要的环境变化。
管理	为用户和 RBAC 以及常规设置等设置提供高级配置。

1.4. 更改密码

这些步骤演示了如何更改密码。

要更改您的 Red Hat Satellite 密码：

1. 点击右上角的用户名。
2. 从菜单中选择 **My Account**。
3. 在 **Current Password** 字段中，输入当前密码。
4. 在 **Password** 字段中，输入新密码。
5. 在 **Verify** 字段中，再次输入新密码。

6. **点** 提交按钮保存新密码。

1.5. 重置管理用户密码

使用以下步骤重置管理密码，以随机生成的字符或设置新的管理密码。

重置管理用户密码：

要将密码重置为随机生成的字符，请完成以下步骤：

1. 登录到安装卫星服务器的基础操作系统。
2. 输入以下命令重置密码：

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

3. 使用此密码在卫星 Web UI 中重置密码。
4. 编辑卫星服务器上的 **~/.hammer/cli.modules.d/foreman.yml** 文件，以添加新密码：

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

除非更新了 **~/.hammer/cli.modules.d/foreman.yml** 文件，否则您无法使用 Hammer CLI 的新密码。

要设置新的管理用户密码：

要将管理用户密码更改为新密码，请完成以下步骤：

1. 登录到安装卫星服务器的基础操作系统。
2. 要设置密码，请输入以下命令：

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

3. 编辑卫星服务器上的 **~/.hammer/cli.modules.d/foreman.yml** 文件，以添加新密码：

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

除非更新了 **~/.hammer/cli.modules.d/foreman.yml** 文件，否则您无法使用 Hammer CLI 的新密码。

1.6. 在登录页面中设置自定义消息

要在登录页面上设置自定义消息：

1. 导航到 **Administer** > **Settings**，然后点 **General** 选项卡。
2. 单击 **Login page footer 文本** 旁边的编辑按钮，并输入要在登录页面上显示所需的文本。例如，此文本可能是您的公司所需的警告消息。
3. 点 **Save**。
4. 从卫星的 Web UI 注销，并验证自定义文本现在显示在卫星版本号下的登录页面中。

第 2 章 启动和停止 RED HAT SATELLITE

Satellite 提供 **satellite-maintain service** 命令，用于从命令行管理卫星服务。这在创建 Satellite 备份时很有用。有关创建备份的详情请参考 第 8 章 *备份 Satellite 服务器和胶囊服务器*。

使用 **satellite-installer** 命令安装 Satellite 后，所有卫星服务都会自动启动并启用。执行以下内容来查看这些服务列表：

```
# satellite-maintain service list
```

要查看正在运行的服务的状态，请执行：

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

要停止 **satellite-maintain** 服务，请执行：

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

要启动 **satellite-maintain** 服务，请执行：

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

要重启 **satellite-maintain** 服务，请执行：

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

第 3 章 从内部 SATELLITE 数据库迁移到外部数据库

安装 Red Hat Satellite 时，**satellite-installer** 命令会将 PostgreSQL 数据库安装到与 Satellite 相同的服务器上。如果您使用默认内部数据库，但希望开始使用外部数据库以帮助进行服务器负载，您可以将内部数据库迁移到外部数据库。

要确认您的 Satellite 服务器是否具有内部或者外部数据库，您可以查询数据库的状态：

对于 PostgreSQL，请输入以下命令：

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

红帽不提供对外部数据库维护的支持或工具。这包括备份、升级和数据库调整。您必须具有自己的数据库管理员才能支持和维护外部数据库。

要从默认内部数据库迁移到外部数据库，您必须完成以下步骤：

1. 第 3.2 节 “为外部数据库准备主机”.准备 Red Hat Enterprise Linux 7 服务器以托管外部数据库。
2. 第 3.3 节 “安装 PostgreSQL”.使用具有所属卫星、Pulp 和 Candlepin 的数据库准备 PostgreSQL。
3. 第 3.4 节 “迁移到外部数据库”.编辑 **satellite-installer** 的参数以指向新数据库，并运行 **satellite-installer**。

3.1. POSTGRESQL 作为外部数据库注意事项

Foreman、Karnish 和 Candlepin 使用 PostgreSQL 数据库。如果要使用 PostgreSQL 作为外部数据库，则以下信息可帮助您确定此选项是否适合您的 Satellite 配置。Satellite 支持 PostgreSQL 版本 12.1。

外部 PostgreSQL 的优点：

- 增加 Satellite 中的可用内存和可用 CPU
- 在 PostgreSQL 数据库上将 **shared_buffers** 的灵活性设置为高数值，而不影响 Satellite 上的其他服务的风险
- 在不影响 Satellite 操作的情况下对 PostgreSQL 服务器系统进行灵活调整

外部 PostgreSQL 的缺陷

- 增加部署复杂性，使故障排除更困难
- 外部 PostgreSQL 服务器是补丁和维护的额外系统
- 如果 Satellite 或 PostgreSQL 数据库服务器遇到硬件或存储故障，卫星无法正常运行
- 如果 Satellite 服务器和数据库服务器之间存在延迟，性能可能会会受到影响

如果您怀疑 Satellite 上的 PostgreSQL 数据库导致性能问题，请使用 Satellite 6 中的信息：如何启用 postgres 查询日志来检测运行速度慢的问题，以确定您是否 有慢的问题查询。需要一秒钟的查询通常是由于大型安装出现性能问题，而移动到外部数据库的查询通常不是帮助。如果您有慢的查询，请联络红帽支持。

3.2. 为外部数据库准备主机

使用最新 Red Hat Enterprise Linux 7 服务器安装一个最新置备的系统，以托管外部数据库。

Red Hat Software Collections 和 Red Hat Enterprise Linux 的订阅不提供将 Satellite 与外部数据库一起使用的正确服务级别协议。您还必须将 Satellite 订阅附加到要用于外部数据库的基础操作系统中。

先决条件

- Red Hat Enterprise Linux 7 服务器必须满足 Satellite 的存储要求。

流程

1. 使用 将 Satellite Infrastructure 订阅附加到服务器中的说明。
2. 禁用所有软件仓库并只启用以下软件仓库：

```
# subscription-manager repos --disable '*'
# subscription-manager repos --enable=rhel-server-rhscl-7-rpms \
--enable=rhel-7-server-rpms --enable=rhel-7-server-satellite-6.10-rpms
```

3.3. 安装 POSTGRESQL

在内部数据库安装过程中，您只能安装与 **satellite-installer** 工具安装的相同版本的 PostgreSQL。只要支持版本，您可以使用 Red Hat Enterprise Linux Server 7 软件仓库或从外部源安装 PostgreSQL。Satellite 支持 PostgreSQL 版本 12.1。

流程

1. 要安装 PostgreSQL，请输入以下命令：

```
# yum install rh-postgresql12-postgresql-server \
rh-postgresql12-syspaths \
rh-postgresql12-postgresql-evr
```

2. 要初始化 PostgreSQL，请输入以下命令：

```
# postgresql-setup initdb
```

3. 编辑 **/var/opt/rh-postgresql12/lib/pgsql/data/postgresql.conf** 文件：

```
# vi /var/opt/rh/rh-postgresql12/lib/pgsql/data/postgresql.conf
```

4. 删除 **#** 并编辑 以侦听入站连接：

```
listen_addresses = '*'
```

5. 编辑 **/var/opt/rh-postgresql12/lib/pgsql/data/pg_hba.conf** 文件：

```
# vi /var/opt/rh/rh-postgresql12/lib/pgsql/data/pg_hba.conf
```

6. 在文件中添加以下行：

```
host  all  all  Satellite_ip/24  md5
```

7. 要启动并启用 PostgreSQL 服务，请输入以下命令：

```
# systemctl start postgresql
# systemctl enable postgresql
```

8. 打开外部 PostgreSQL 服务器上的 **postgresql** 端口：

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

9. 切换到 **postgres** 用户并启动 PostgreSQL 客户端：

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

10. 创建三个数据库和专用角色：一个用于 Satellite，一个用于 Candlepin，另一个用于 Pulp：

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

11. 退出 **postgres** 用户：

```
# \q
```

12. 从卫星服务器，测试您可以访问数据库。如果连接成功，命令会返回 **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"
# PGPASSWORD='Pulpcore_Password' psql -h postgres.example.com -p 5432 -U pulp -d
pulpcore -c "SELECT 1 as ping"
```

3.4. 迁移到外部数据库

备份并传输现有数据，然后使用 **satellite-installer** 命令配置卫星以连接到外部 PostgreSQL 数据库服务器。

先决条件

- 您已在 Red Hat Enterprise Linux 服务器中安装和配置了 PostgreSQL 服务器。

流程

1. 在 Satellite 服务器中停止 **satellite-maintain** 服务：

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

2. 启动 **PostgreSQL** 服务：

```
# systemctl start postgresql
```

3. 备份内部数据库：

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

4. 将数据传送到新外部数据库中：

```
PGPASSWORD='Foreman_Password' pg_restore -h postgres.example.com -U foreman -d
foreman < /var/migration_backup/foreman.dump
PGPASSWORD='Candlepin_Password' pg_restore -h postgres.example.com -U candlepin -
d candlepin < /var/migration_backup/candlepin.dump
PGPASSWORD='Pulpcore_Password' pg_restore -h postgres.example.com -U pulp -d
pulpcore < /var/migration_backup/pulpcore.dump
```

5. 使用 **satellite-installer** 命令更新 Satellite 以指向新数据库：

```
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 \
  --foreman-proxy-content-pulpcore-manage-postgresql false \
  --foreman-proxy-content-pulpcore-postgresql-host postgres.example.com \
  --foreman-proxy-content-pulpcore-postgresql-db-name pulpcore \
  --foreman-proxy-content-pulpcore-postgresql-password Pulpcore_Password
```

第 4 章 使用 ANSIBLE COLLECTIONS 管理 SATELLITE

卫星 Ansible Collections 是与卫星 API 交互的一组 Ansible 模块。您可以使用 Satellite Ansible Collections 管理和自动化卫星的许多方面。

4.1. 从 RPM 安装 SATELLITE ANSIBLE 模块

使用此流程安装 Satellite Ansible 模块。

前提条件

- 确保启用了 Ansible 2.9 或更高版本的存储库，并且 ansible 软件包已更新：

```
# subscription-manager repos --enable rhel-7-server-ansible-2.9-rpms
# satellite-maintain packages update ansible
```

流程

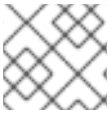
- 使用以下命令安装 RPM：

```
# satellite-maintain packages install ansible-collection-redhat-satellite
```

4.2. 查看 SATELLITE ANSIBLE 模块

您可以通过列出以下目录的内容来查看已安装的 Satellite Ansible 模块：

```
# ls /usr/share/ansible/collections/ansible_collections/redhat/satellite/plugins/modules/
```



注意

编写本文时，**ansible-doc -l** 命令尚未列出集合。

另外，您还可以查看 Satellite Ansible 模块和其他相关信息的完整列表，网址为 https://console.redhat.com/ansible/automation-hub/redhat/satellite/docs

所有模块都采用 **redhat.satellite** 命名空间，格式为 **redhat.satellite._module_name_**。例如，要显示 **activation_key** 模块的信息，请输入以下命令：

```
$ ansible-doc redhat.satellite.activation_key
```

第 5 章 管理用户和角色

用户使用系统为个人定义一组详细信息。用户可以与组织和环境关联，以便在创建新实体时，自动使用默认设置。用户也可以附加一个或多个 *角色*，授予他们查看和管理组织和环境的权限。有关使用用户的更多信息，请参阅 第 5.1 节 “用户管理”。

您可以通过将多个用户组织到用户组来同时管理多个用户的权限。用户组本身可以进一步分组以创建权限层次结构。有关创建用户组的更多信息，请参阅 第 5.3 节 “创建和管理用户组”。

角色定义了一组权限和访问级别。每个角色都包含多个 *权限过滤器*，用于指定角色允许的操作。操作按照 *资源类型* 分组。创建了角色后，可将用户和用户组与该角色关联。这样，您可以为大用户组分配相同的权限集。Red Hat Satellite 提供了一组预定义的角色，还可创建自定义角色和权限过滤器，如 第 5.4 节 “创建和管理角色” 所述。

5.1. 用户管理

作为管理员，您可以创建、修改和删除 Satellite 用户。您还可以通过分配不同 *角色* 来为用户或一组用户配置访问权限。

5.1.1. 创建用户

使用此流程创建用户。要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

流程

要创建用户，请完成以下步骤：

1. 进入 **Administer** > **Users**。
2. 单击 **创建用户**。
3. 在 **Login** 项中输入用户的用户名。
4. 在 **Firstname** 和 **Lastname** 字段中输入用户的真实名字和姓氏。
5. 在 **Mail** 字段中，输入用户的电子邮件地址。
6. 在 **Description** 字段中，添加新用户的描述。
7. 从 **Language** 列表中选择用户的具体语言。
8. 从 **Timezone** 列表中选择该用户的时区。
   默认情况下，卫星服务器使用用户浏览器的语言和时区设置。
9. 为该用户设置密码：
   a. 从 **Authorized by** 列表中，选择用户通过身份验证的来源。
      - **INTERNAL** ：允许用户在卫星服务器中管理。
      - **EXTERNAL** ：配置外部身份验证，如 第 13 章 *配置外部身份验证* 所述。
   b. 在 **Password** 字段和 Verify 字段中输入用户 **的初始密码**。
10. 单击 **Submit** 以创建用户。

CLI 过程

- 运行以下命令来创建用户：

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

auth-source-id 1 设置意味着用户在内部进行身份验证，您可以将外部身份验证源指定为替代选择。添加 **--admin** 选项，以向用户授予管理员特权。不需要指定机构 ID，您可以使用 **update** 子命令修改用户详情。

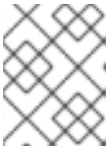
有关用户相关子命令的更多信息，请输入 **hammer 用户 --help**。

5.1.2. 为用户分配角色

使用此流程为用户分配角色。要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

流程

1. 进入 **Administer** > **Users**。
2. 单击要分配一个或多个角色的用户的用户名。



注意

如果某个用户帐户没有被列出，请检查您是否当前查看正确的机构。若要列出卫星中的所有用户，请单击 Default Organization，然后单击 Any Organization。

3. **单击位置选项卡，如果不分配，则选择一个位置。**
4. **单击 Organizations 选项卡，然后检查是否分配了组织。**
5. **单击 Roles 选项卡，以显示可用角色的列表。**
6. **从 Roles 列表中选择要分配的角色。**
   要授予所有可用权限，请选中 Admin 复选框。
7. **点 Submit。**

若要查看分配给用户的角色，请单击 Roles 选项卡；分配的角色列在 Selected items 下。要删除分配的角色，可在 Selected items 中单击角色名称。

CLI 过程

要为用户分配角色，请输入以下命令：

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

5.1.3. 模拟不同的用户帐户

管理员可以以不同的用户身份临时登录卫星 Web UI 来模拟其他经过身份验证的用户用于测试和故障排除目的。在模拟其他用户时，管理员具有访问模拟用户可以访问权限，包括同一菜单。

创建审计是为了记录管理员在模拟另一个用户时执行的操作。但是，管理员在模拟另一用户期间执行的所有操作都会记录被模拟用户执行的。

先决条件

- 确保您已以具有 Satellite 管理员权限的用户身份登录卫星 Web UI。

流程

要模拟不同的用户帐户，请完成以下步骤：

1. 在 Satellite Web UI 中，导航到 Administer > Users。
2. 在您要模拟的用户右侧，从 Actions 列中的列表中选择 Impersonate。

当要停止模拟会话时，在主菜单右上角点击模拟图标。

5.2. SSH 密钥管理

向用户添加 SSH 密钥允许在置备过程中部署 SSH 密钥。

有关在置备过程中部署 SSH 密钥的信息，请参阅 *《部署指南》* 中的 部署 SSH 密钥。

有关 SSH 密钥和 SSH 密钥创建的详情，请参考 *Red Hat Enterprise Linux 7 系统管理员指南中的使用基于 SSH 的身份验证*。

5.2.1. 管理用户 SSH 密钥

使用这个流程为用户添加或删除 SSH 密钥。要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

先决条件

确保您已作为 Red Hat Satellite 的 Admin 用户或启用了 *create_ssh_key* 权限的用户登录到 web UI，从而添加 SSH 密钥和 *destroy_ssh_key* 权限。

流程

1. 进入 Administer > Users。
2. 从 Username 列中，单击所需用户的用户名。
3. 点 SSH Keys 选项卡。
   - 添加 SSH 密钥
     i. 在剪贴板中准备公共 SSH 密钥的内容。
     ii. 点 Add SSH Key。
     iii. 在 Key 字段中，粘贴剪贴板中的公共 SSH 密钥内容。
     iv. 在 Name 字段中输入 SSH 密钥的名称。
     v. 点 Submit。

- 删除 SSH 密钥
  i. 点要删除的 SSH 密钥行上的 Delete。
  ii. 在确认提示中点 OK。

CLI 过程

要向用户添加 SSH 密钥，您必须指定公共 SSH 密钥文件的路径，或者指定复制到剪贴板中的公共 SSH 密钥的内容。

- 如果您有公共 SSH 密钥文件，请输入以下命令：

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

- 如果您有公共 SSH 密钥内容，请输入以下命令：

```
# hammer user ssh-keys add \
--user-id user_id \
--name key_name \
--key ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNtYAAABBBHHS2KmNyIYa27Qaa7
EHp+2l99ucGStx4P77e03ZvE3yVRJEFikpoP3MJtYYfle8k 1/46MTlZo9CPTX4CYUHeN8=
host@user
```

要从用户中删除 SSH 密钥，请输入以下命令：

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

要查看附加到用户的 SSH 密钥，请输入以下命令：

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

要列出附加到用户的 SSH 密钥，请输入以下命令：

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

5.3. 创建和管理用户组

5.3.1. 用户组

使用 Red Hat Satellite，您可以为用户组分配权限。您还可以创建用户组，作为其他用户组的集合。如果使用外部身份验证源，您可以将 Satellite 用户组映射到外部用户组，如 第 13.4 节 “配置外部用户组” 所述。

用户组在组织上下文中定义，这意味着您必须选择一个机构，然后才能访问用户组。

5.3.2. 创建用户组

使用此流程来创建用户组。

流程

1. 进入 Administer > User Groups。
2. 点 Create User group。
3. 在 User Group 选项卡中，指定新用户组的名称并选择组成员：
   - 从 User Groups 列表中选择之前创建的用户组。
   - 从 Users 列表中选择用户。
4. 在角色 选项卡中，选择您要分配给用户组的角色。或者，选择 Admin 复选框来分配所有可用权限。
5. 点 Submit。

CLI 过程

- 要创建用户组，请输入以下命令：

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

5.3.3. 删除用户组

使用卫星 Web UI 删除用户组。

流程

1. 进入 Administer > User Groups。
2. 点击您要删除的用户组右侧的 Delete。
3. 在出现的警报框中，单击 OK 以删除用户组。

5.4. 创建和管理角色

Red Hat Satellite 提供了一组具有足够标准任务的预定义角色，如 第 5.4.7 节 “Satellite 中可用的预定义角色” 中列出的。也可以配置自定义角色，并为它们分配一个或多个权限过滤器。权限过滤器定义允许进行某些资源类型的操作。某些 Satellite 插件会自动创建角色。

5.4.1. 创建角色

使用此流程创建角色。

流程

1. 导航到 Administer > Roles。
2. 点 Create Role。
3. 为角色提供一个 Name。

4. 单击 Submit 以保存您的新角色。

CLI 过程

运行以下命令来创建角色：

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

为满足其目的，角色必须包含权限。创建角色后，进入 第 5.4.3 节 “为角色添加权限”。

5.4.2. 克隆角色

使用卫星 Web UI 克隆角色。

流程

1. 导航到 Administer > Roles，然后从所需角色右侧的下拉菜单中选择 Clone。
2. 为角色提供一个 Name。
3. 单击 Submit 以克隆角色。
4. 点击克隆角色的名称并导航到 过滤器。
5. 根据需要编辑权限。
6. 单击 Submit 以保存您的新角色。

5.4.3. 为角色添加权限

使用这个流程为角色添加权限。要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

流程

1. 导航到 Administer > Roles。
2. 从所需角色右侧的下拉列表中选择 Add Filter。
3. 从下拉列表中选择 Resource type。*(Miscellaneous)* 组收集不与任何资源组关联的权限。
4. 点击您要从 Permission 列表中选择的权限。
5. 根据所选的 资源类型，您可以选择或取消选择 Unlimited 和 Override 复选框。默认选择 无限 复选框，这表示在所选类型的所有资源中应用该权限。当您禁用 unrestricted 复选框 时，Search 字段会自动激活。在此字段中，您可以使用 Red Hat Satellite 6 搜索语法指定进一步过滤。详情请查看 第 5.5 节 “细粒度权限过滤”。启用 Override 复选框时，您可以添加附加位置和组织，以允许该角色访问附加位置和机构中的资源类型；您还可以从资源类型中删除已经关联的位置和机构来限制访问权限。
6. 点击 Next。
7. 单击 Submit 以保存更改。

CLI 过程

1. 列出所有可用权限：

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

2. 为角色添加权限：

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

有关角色和权限参数的更多信息，请输入 hammer 角色 --help 和 hammer 过滤器 --help 命令。

5.4.4. 查看角色的权限

使用卫星 Web UI 查看角色的权限。

流程

1. 导航到 Administer > Roles。
2. 点所需角色右侧的 Filters 以进入 Filters 页面。

Filters 页面包含分配给根据资源类型分组的角色的权限表。也可以生成可在 Satellite 系统中使用的权限和操作的完整表。具体步骤请查看 第 5.4.5 节 “创建完全权限表”。

5.4.5. 创建完全权限表

使用 Satellite CLI 创建权限表。

流程

1. 确保安装了所需的软件包。在 Satellite 服务器中执行以下命令：

```
# satellite-maintain packages install foreman-console
```

2. 使用以下命令启动 Satellite 控制台：

```
# foreman-rake console
```

将以下代码插入到控制台中：

```
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)
```

以上语法创建了权限表，并将其保存到 /tmp/table.html 文件中。

3. 按 Ctrl + D 退出 Satellite 控制台。在 /tmp/table.html 的第一行中插入以下文本：

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

在 /tmp/table.html 末尾附加以下文本：

```
</table>
```

4. **在 Web 浏览器中打开 /tmp/table.html，以查看表。**

5.4.6. 删除角色

使用卫星 Web UI 删除角色。

流程

1. **导航到 Administer > Roles。**
2. **从要删除的角色右侧的下拉列表中选择 Delete。**
3. **在出现的警报框中，单击 OK 以删除该角色。**

5.4.7. Satellite 中可用的预定义角色

角色	角色提供的权限 [a]
访问 Insights Admin	添加并编辑 Insights 规则。
访问 Insights Viewer	查看 Insight 报告.
Ansible Roles Manager	在主机和主机组上扮演角色。查看、销毁和导入 Ansible 角色。查看、编辑、创建、销毁和导入 Ansible 变量。
Ansible Tower 清单阅读器	查看事实、主机和主机组。
书签管理器	创建、编辑和删除书签。
引导磁盘访问	下载引导磁盘。
Compliance manager	查看、创建、编辑和删除 SCAP 内容文件、合规性策略和定制文件。查看合规性报告。
Compliance viewer	查看合规性报告。
创建 ARF 报告	创建合规性报告。
默认角色	每个用户授予的权限集，对任何其他角色无关。
Discovery Manager	查看、调配、编辑和销毁发现的主机，并管理发现规则。

角色	角色提供的权限 [a]
Discovery Reader	查看主机和发现规则。
编辑主机	查看、创建、编辑、销毁和构建主机。
编辑分区表	查看、创建、编辑和销毁分区表。
Manager（管理者）	角色类似于管理员，但没有权限编辑全局设置。在 Satellite Web UI 中，可在 **Administer** > **Settings** 下找到全局设置。
机构管理员	每个机构定义的管理员角色。该角色对其他组织中的资源没有可见性。
红帽访问日志	查看日志查看器和日志。
远程执行管理器	角色具有完整的远程执行权限，包括修改作业模板。
远程执行用户	运行远程执行作业。
网站管理器	Manager 角色的约束版本。
系统管理员	• 在 **Administer** > **Settings** 中编辑全局设置 • 查看、创建、编辑和销毁用户、用户组和角色。 • 查看、创建、编辑、销毁和分配组织和位置，但不能查看其中的资源。 具有此角色的用户可以创建用户，并将所有角色分配给他们。因此，请确保只为受信任的用户授予此角色。
任务管理器	查看和编辑 Satellite 任务。
任务读取器	只能查看 Satellite 任务的角色。
Viewer	被动角色，提供查看卫星结构、日志、报告和统计元素的配置的功能。
查看主机	只能查看主机的角色。
virt-who Manager	具有完整的 virt-who 权限的角色。
virt-who Reporter	将 virt-who 生成的报告上传到 Satellite。如果您手动配置 virt-who，且需要具有有限 virt-who 权限的用户角色。
virt-who Viewer	查看 virt-who 配置。具有此角色的用户可以使用现有 virt-who 配置部署 virt-who 实例。

[a] 特权用户可以查看与预定义角色关联的操作集合，如 所述 第 5.4.4 节 “查看角色的权限”

5.5. 细粒度权限过滤

5.5.1. 粒度权限过滤器

如 第 5.4.3 节 “为角色添加权限” 所述，Red Hat Satellite 提供了将配置的用户权限限制为资源类型的选定实例的能力。这些细致的过滤器是对 Satellite 数据库的查询，受到大多数资源类型的支持。

5.5.2. 创建 Granular Permission Filter

使用此流程创建精细的过滤器。要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

Satellite 不应用搜索条件来创建操作。例如，在搜索字段中使用 *name = "Default Location"* 表达式限制 *create_locations* 操作不会阻止用户为新建的位置分配自定义名称。

流程

在 Edit Filter 页面上的 Search 字段中指定一个查询。取消选择该字段的 unrestricted 复选框为 active。查询有以下形式：

```
field_name operator value
```

- *field_name* 标记要查询的字段。可用字段名称的范围取决于资源类型。例如，*Partition Table* 资源类型提供 *系列*、*布局* 和 *名称* 作为查询参数。
- *Operator* 指定 *field_name* 和 *值* 之间的比较类型。如需了解适用 Operator 的概述信息，请参阅 第 5.5.4 节 “Granular Search 支持的 Operator”。
- *value* 是用于过滤的值。这可以是机构的名称。支持两种通配符字符：下划线(_)提供单字符替换，而百分比符号(%)替换零个或更多字符。

对于大多数资源类型，Search 字段提供建议可用参数的下拉列表。此列表显示在搜索字段中。对于很多资源类型，您可以使用逻辑运算符（如 *和*）而不是 *运算符* 来组合查询。

CLI 过程

- 要创建细致的过滤器，使用 **--search** 选项输入 **hammer** 过滤器 **create** 命令来限制权限过滤器，例如：

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

此命令添加到 **qa-user** 角色中具有查看、创建、编辑和销毁内容视图的权限，它们仅应用于以 **ccv** 开始的名称的 **Content Views**。

5.5.3. 使用 Granular Permission Filters 的示例

作为管理员，您可以允许所选用户对环境路径的某些部分进行更改。通过以下过滤器，您可以在应用程序生命周期的开发阶段处理内容，但内容一旦推送到生产环境后便无法访问。

5.5.3.1. 为主机资源类型应用权限

以下查询将为 **Host** 资源类型指定的任何权限应用到名为 **host-editors** 的组中主机。

```
hostgroup = host-editors
```

以下查询会返回记录，其中 name 与 XXXX、Yyyy 或 zzzz 示例字符串匹配：

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

您还可以限制所选环境的权限。要做到这一点，在 Search 字段中指定环境名称，例如：

```
Dev
```

您可以使用 Search 字段中的粒度权限过滤器将用户权限限制为特定的机构或位置。但是，有些资源类型提供 GUI 替代方案，即提供 位置 和机构选项卡的 覆盖 复选框。在这些标签页中，您可以从可用的机构和位置列表中选择。请参阅 第 5.5.3.2 节 “创建机构特定管理器角色”。

5.5.3.2. 创建机构特定管理器角色

使用卫星 UI 创建仅限于名为 org-1 的单一组织的管理角色。

流程

1. 导航到 Administer > Roles。
2. 克隆现有的 机构管理员 角色。从 过滤器 按钮旁边的下拉列表中选择 Clone。然后会提示您输入克隆角色的名称，如 org-1 admin。
3. 单击所需的位置和组织，将它们与角色相关联。
4. 单击 Submit 以创建角色。
5. 单击 org-1 admin，然后单击 Filters 以查看所有关联的过滤器。对于大多数用例，默认过滤器都可以正常工作。但是，您可以选择点击 Edit 来更改每个过滤器的属性。对于某些过滤器，如果您希望该角色能够访问附加位置和机构中的资源，则可以启用 Override 选项。例如，通过选择 Domain 资源类型、Override 选项，然后使用 Locations 和 Organizations 选项卡的其他位置和机构访问额外位置和没有与此角色关联的机构中的域。您还可以单击 New filter，将新过滤器与此角色相关联。

5.5.4. Granular Search 支持的 Operator

表 5.1. 逻辑 Operator

Operator	描述
和	组合搜索条件。
not	negates 表达式。
具有	对象必须具有指定的属性。

表 5.2. 符号链接 Operator

Operator	描述

=	*等于*。对文本字段区分大小写的相等性比较。
!=	*不等于*。= 运算符的 inversion。
~	*比如*。搜索文本字段不区分大小写。
!~	*不喜欢*。~ 运算符的 inversion。
^	*在* 中。对文本字段区分大小写的搜索的等性比较。这会生成不同的 SQL 查询，与比较*相等*，并对多个值比较效率更高。
!^	*不在 中*。^ 运算符的 inversion。
>, >=	*大于*，*大于或等于*。仅支持数字字段。
<, ⇐	*小于*，*小于或等于*。仅支持数字字段。

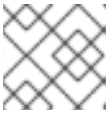
第 6 章 配置电子邮件通知

您可以配置 Satellite，以将电子邮件消息发送到卫星中注册的单独用户。如果出现，红帽卫星将电子邮件发送到已添加到帐户的电子邮件地址。用户可以在卫星 Web UI 右上角单击其名称，然后选择 My account 来编辑电子邮件地址。

从卫星 Web UI 配置用户的电子邮件通知。

流程

1. 进入 Administer > Users。
2. 点您要编辑的用户的 Username。
3. 在 User 选项卡中，验证 Mail 字段的值。电子邮件通知将在此字段中发送到地址。
4. 在 "电子邮件首选项" 选项卡中，选择 " 邮件启用 "。
5. 使用通知类型旁边的下拉菜单选择您希望用户接收的通知。



注意

可以通过在 Mail Query 文本框中输入所需的查询来过滤 Audit Summary 通知。

6. 点 Submit。
用户将开始收到通知电子邮件。

6.1. 测试电子邮件发送

要验证电子邮件的发送，请向用户发送测试电子邮件。如果电子邮件被发送，则设置正确无误。

流程

1. 在 Satellite Web UI 中，导航到 Administer > Users。
2. 点用户名。
3. 在 电子邮件首选项 选项卡中，单击 Test email。
立即向用户的电子邮件地址发送测试电子邮件消息。

如果发送了电子邮件，则验证已完成。否则，您必须执行以下诊断步骤：

a. 验证用户的电子邮件地址。

b. 验证卫星服务器的电子邮件配置。

c. 检查防火墙和邮件服务器日志。

6.2. 测试电子邮件通知

要验证用户是否已正确订阅了通知，请手动触发通知。

流程

- 要触发通知，请执行以下命令：

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

使用以下任一方式替换 **frequency** ：

- **daily**
- **weekly**
- **monthly**

这会触发为所有订阅的用户的指定频率调度的所有通知。如果每个订阅的用户都收到通知，验证会成功。

注意

目前不支持向单独的用户发送手动触发通知。

6.3. 通知类型

以下是 **Satellite** 创建的通知：

- *审计摘要* ：由卫星服务器审计的所有活动的摘要。
- *主机构建* ：主机构建时发送的通知。
- *主机勘误公告* ：用户管理的主机的总和可安装勘误表。
- **OpenSCAP** 策略摘要 ： **OpenSCAP** 策略报告及其结果的摘要。
- *提升勘误表* ：仅在内容视图提升后发送的通知。它包含可用于注册到提升内容视图的主机的勘误表摘要。这样，用户可以监控哪些更新已应用到哪些主机。
- **Puppet** 错误状态 ：在主机报告了与 **Puppet** 相关的错误后发送的通知。
- **Puppet** 摘要 ：**Puppet** 报告的摘要。
- *同步勘误表* ：仅在同步存储库后发送的通知。它包含由同步引入的新勘误的摘要。

6.4. 更改主机的电子邮件通知设置

卫星可为主机发送事件通知到主机的注册所有者。

您可以将卫星配置为向个人用户或用户组发送电子邮件通知。当设置为用户组时，订阅到电子邮件类型的所有组成员都会收到消息。

要查看主机的通知状态，请导航到 **Hosts > All Hosts**，再点击您要查看的主机。在主机详情页面中，点 **Additional Information** 选项卡，您可以查看电子邮件通知状态。

接收主机的电子邮件通知会很有用，但如果您希望收到频繁错误（例如，由于您正在使用的已知问题或错误），则还不堪重负。

要更改主机的电子邮件通知设置，请完成以下步骤。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > All Hosts，再选择具有您要更改的通知设置的主机。
2. 选择主机的复选框，从 Select Action 列表中，选择 Enable Notifications 或 Disable Notifcations，具体取决于您需要的内容。

第 7 章 管理安全合规性

安全合规管理是定义安全策略、审计符合这些策略并解决不合规实例的持续流程。任何非合规均根据机构的配置管理策略进行管理。安全策略涵盖了从主机特定于行业范围的范围，因此需要其定义灵活性。

7.1. 安全内容自动化协议

Satellite 6 使用安全内容自动化协议(SCAP)来定义安全配置策略。例如，安全策略可能会指定针对运行 Red Hat Enterprise Linux 的主机，不允许通过 SSH 登录 **root** 帐户。借助 Satellite 6，您可以调度管理所有主机上的合规性审计和报告。有关 SCAP 的更多信息，请参阅 Red Hat Enterprise Linux 7 安全指南。

7.1.1. SCAP 内容

SCAP 内容是一个数据流格式，包含主机要检查的配置和安全基准。检查清单以可扩展的清单配置描述格式(XCCDF)和开放漏洞和评估语言(OVAL)中的漏洞描述。检查清单项目，也称为规则表示系统项目所需的配置。例如，您可以指定没有人可以使用 **root** 用户帐户通过 SSH 登录主机。可将规则分组到一个或多个配置集中，允许多个配置集共享规则。SCAP 内容同时由规则和配置集组成。

您可以创建 SCAP 内容或从供应商获取它。在 scap-security-guide 软件包中，为 Red Hat Enterprise Linux 提供了支持的配置集。创建 SCAP 内容超出了本指南的范围，但请参见 Red Hat Enterprise Linux 7 安全指南 来获得有关如何下载、部署、修改和创建您自己的内容的信息。

由 Satellite 6 的 OpenSCAP 组件提供的默认 SCAP 内容取决于 Red Hat Enterprise Linux 的版本。Red Hat Enterprise Linux 7 中已安装 Red Hat Enterprise Linux 6 和 Red Hat Enterprise Linux 7 的内容。

7.1.2. XCCDF Profile

XCCDF 配置集是一个检查主机或主机组的清单。创建配置集来验证与行业标准或自定义标准的合规性。

通过 Satellite 6 提供的配置集从 OpenSCAP 项目 获取。

7.1.2.1. 列出可用的 XCCDF 配置集

在 Satellite UI 中，列出可用的 XCCD 配置集。

流程

- 进入 **Hosts > SCAP contents**。

7.2. 配置 SCAP 内容

7.2.1. 导入 OpenSCAP Puppet 模块

注意

如果不使用 Puppet 在主机上配置 OpenSCAP 审计，您可以跳过这个过程。

要使用 OpenSCAP 审计主机，您必须首先导入 Puppet 环境。Puppet 环境包含您必须分配给每个主机的 Puppet 类，以部署 OpenSCAP 配置。

您必须将您要审计的每个主机与卫星 Web UI 中的 Puppet 环境关联。

流程

1. 在 Satellite Web UI 中，导航到 Configure > Environments。
2. 单击 Import environments from satellite.example.com。
3. 选择与您要审计的主机关联的 Puppet 环境复选框。
   如果没有 Puppet 环境，请选择 production 环境复选框。默认情况下，在生产环境中为 OpenSCAP 所需的 Puppet 类是。
4. 点 Update。

7.2.2. 加载默认 OpenSCAP 内容

在 CLI 中，加载默认的 OpenScap 内容。

流程

- 使用 **foreman-rake** 命令：

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

7.2.3. 额外的 SCAP 内容

您可以将额外的 SCAP 内容上传到卫星服务器中，可以是您自己创建的内容，也可以在其他地方获得。在策略中应用 SCAP 内容前，必须将 SCAP 内容导入到卫星服务器中。例如，Red Hat Enterprise Linux 7.2 软件仓库中提供的 **scap-security-guide** RPM 软件包包括支付卡行业数据安全标准(PCI-DSS)版本 3 的配置集。您可以将此内容上传到卫星服务器中，即使它没有运行 Red Hat Enterprise Linux 7.2，因为内容不特定于操作系统版本。

7.2.3.1. 上传额外 SCAP 内容

在卫星 Web UI 中，上传额外的 SCAP 内容。

流程

1. 导航到 Hosts > SCAP contents，再单击 New SCAP Content。
2. 在 title 文本框中输入 标题。
   示例： **RHEL 7.2 SCAP** 内容.
3. 单击 Choose file，导航到包含 SCAP 内容文件的位置，然后选择 Open。
4. 点 Submit。

如果成功载入 SCAP 内容文件，则会显示类似于 **Successfully created RHEL 7.2 SCAP Contents** 的消息，并且会包括新标题。

7.3. 管理合规策略

7.3.1. 合规策略

一个调度的审计（也称为 合规策略 ）是一个调度任务，用于检查指定的主机是否与 XCCDF 配置集相符。扫描的计划由卫星服务器指定，扫描则在主机上执行。扫描完成后，将以 XML 格式生成资源报告文件

(ARF) 并上传到卫星服务器。您可以在合规性策略控制面板中查看扫描结果。合规策略不会对扫描的主机进行任何更改。SCAP 内容包含多个包含关联规则的配置集，但默认情况下不包含策略。

7.3.2. 创建合规策略

使用 Satellite 6，您可以创建一个合规策略来扫描您的内容主机，以确保主机保持符合您的安全要求。

您可以使用 Puppet 或 Ansible 将合规性策略部署到您的主机上。请注意，Puppet 每 30 分钟运行一次。如果分配新策略，则下一个 Puppet 运行会将策略同步到主机。但是 Ansible 不会执行调度运行。要添加新策略，您必须手动或使用远程执行运行 Ansible 角色。有关远程执行的更多信息，请参阅 管理主机 指南中的配置和设置远程作业。

先决条件

在开始之前，您必须决定要使用 Puppet 还是 Ansible 部署。

- 对于 Puppet 部署，请确保您要审计的每个主机都与 Puppet 环境关联。更多信息请参阅 第 7.2.1 节 “导入 OpenSCAP Puppet 模块”。
- 对于 Ansible 部署，请确保导入 **foreman.foreman_scap_client** Ansible 角色。有关导入 Ansible 角色的更多信息，请参阅配置 Satellite 中的 Ansible 入门以使用 Ansible。

流程

1. 导航到 **Hosts > Policies**，并选择您要手动、Ansible 或 Puppet 部署。
2. 输入此策略的名称、描述（可选），然后单击 下一步。
3. 选择要应用的 SCAP Content 和 XCCDF Profile，然后单击 **Next**。
   在 BZ#1704582 得到解决之前，请注意 **Default XCCDF Profile** 可能会返回空报告。
4. 指定应用策略时调度的时间，然后点 **Next**。
   从 **Period** 列表中选择 **Weekly**、**Monthly** 或 **Custom**。
   - 如果选择 **Weekly**，也可从 **Weekday** 列表中选择一周的所需日期。
   - 如果您选择了 **Monthly**，在月的几号中指定下月的所需日期。
   - 如果您选择 **Custom**，在 **Cron line** 字段中输入有效的 Cron 表达式。
     Custom 选项允许策略调度的灵活性大于周或几 月 选项。
5. 选择要应用策略的位置，然后点 **Next**。
6. 选择要应用策略的组织，然后点 **Next**。
7. 选择要应用该策略的主机组，然后单击 **Submit**。

当 Puppet 代理在属于所选主机组或策略所应用到的主机上运行时，将安装 OpenSCAP 客户端，以及添加策略指定调度的 Cron 作业。**SCAP Content** 选项卡提供 SCAP 内容文件的名称，该文件将发送到所有目标主机上的 **/var/lib/openscap/content/** 目录中。

7.3.3. 查看合规策略

您可以预览特定 OpenSCAP 内容和配置文件组合应用的规则。这在规划策略时很有用。

在卫星 Web UI 中，查看合规性策略。

流程

1. 进入 Hosts > Policies。
2. 单击 Show Guide。

7.3.4. 编辑合规策略

在卫星 Web UI 中，编辑合规性策略。

流程

1. 进入 Hosts > Policies。
2. 从策略名称右侧的下拉列表中，选择 Edit。
3. 编辑必要的属性。
4. 点 Submit。

当其 Puppet 代理对卫星服务器进行下一次检查以进行更新时，会将编辑的策略应用到主机。默认情况下，每 30 分钟发生一次。

7.3.5. 删除合规策略

在卫星 Web UI 中，删除现有策略。

1. 进入 Hosts > Policies。
2. 从策略名称右侧的下拉列表中，选择 Delete。
3. 在确认消息中点 OK。

7.4. 定制文件

定制文件允许自定义现有 OpenSCAP 策略，而无需对策略进行分叉或重写。您可以在创建或更新策略时将定制文件分配给策略。

您可以使用 SCAP Workbench 创建定制文件。有关使用 SCAP Workbench 工具的更多信息，请参阅为您的用例自定义 SCAP 安全指南。

7.4.1. 上传定制文件

在卫星 Web UI 中，上传 Tailoring 文件。

流程

1. 导航到 Hosts > Compliance - Tailoring Files，再单击 New Tailoring File。
2. 在 Name 文本框中输入名称。
3. 单击 Choose File，导航到包含 SCAP DataStream Tailoring File 的位置，然后选择 Open。
4. 单击 Submit 以上传所选的 Tailoring File。

7.4.2. 将定制文件分配给策略

在卫星 Web UI 中，将 Tailoring 文件分配给策略。

流程

1. 进入 Hosts > Compliance - Policies。
2. 如果有现有的 Compliance Policies，则单击 New Policy 或 New Compliance Policy。
3. 在 Name 文本框中输入名称，然后单击下一步。
4. 从下拉菜单中选择 Scap 内容。
5. 从下拉菜单中选择 XCCDF Profile。
6. 从下拉菜单中选择 Tailoring File。
7. 从下拉菜单选择 XCCDF Profile in Tailoring File。
   选择 XCCDF Profile 非常重要，因为 Tailoring Files 可以包含多个 XCCDF 配置集。
8. 点击 Next。
9. 从下拉菜单中选择一个 时段。
10. 从下拉菜单中选择 Weekday，然后单击 Next。
11. 选择一个 Location 以将它移到已 选项窗口，然后单击 Next。
12. 选择一个 组织 来将它移到已 选项窗口，然后单击 Next。
13. 选择一个 Hostgroup 以将它移到已 选项 窗口，然后单击 Submit。

7.5. 为 OPENSCAP 配置主机组

使用这个流程为主机组配置所有 OpenSCAP 要求。

OpenSCAP 设置概述

您必须在卫星服务器上完成以下任务，以便为主机组分配必要的组件：

- 在 Capsule 上启用 OpenSCAP。如需更多信息，请参阅安装 胶囊服务器 指南中的在外部胶囊上启用 OpenSCAP。
- 分配 OpenSCAP 胶囊。
- 分配包含用于部署 OpenSCAP 策略的 Puppet 类的 Puppet 环境。
- 分配 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类。
- 分配您要添加的任何合规策略。

有关创建和管理主机的详情，请参考 管理主机 指南。

流程

1. 在 Satellite Web UI 中，导航到 Configure > Host Groups，然后创建一个主机组，或者点击您要为 OpenSCAP 报告配置的主机组。
2. 在 Puppet Environment 列表中，选择包含 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类的 Puppet 环境。
3. 在 OpenSCAP Capsule 列表中，选择启用的 OpenSCAP 的胶囊。
4. 单击 Puppet Classes 选项卡，再添加 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类。
5. 点 Submit 保存您的更改。
6. 进入 Hosts > Policies。
7. 选择您要分配给主机组的策略。
8. 点 主机组选项卡。
9. 在 Host Groups 列表中，选择您要分配给此策略的多个主机组。
10. 点 Submit 保存您的更改。

7.6. 为 OPENSCAP 配置主机

使用这个流程为主机配置所有 OpenSCAP 要求。

OpenSCAP 设置概述

您必须在裸机上完成以下任务来为主机分配必要的组件：

- 在 Capsule 上启用 OpenSCAP。如需更多信息，请参阅安装 胶囊服务器 指南中的在外部胶囊上启用 OpenSCAP。
- 分配 OpenSCAP 胶囊。
- 分配包含用于部署 OpenSCAP 策略的 Puppet 类的 Puppet 环境。
- 分配 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类。
- 分配您要添加的任何合规策略。

有关创建和管理主机的详情，请参考 管理主机 指南。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > All Hosts，然后在您要为 OpenSCAP 报告配置的主机上选择 Edit。
2. 在 Puppet Environment 列表中，选择包含 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类的 Puppet 环境。
3. 在 OpenSCAP Capsule 列表中，选择启用的 OpenSCAP 的胶囊。
4. 单击 Puppet Classes 选项卡，再添加 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类。

5. 要添加合规策略，请导航到以下位置之一：
6. 进入 **Hosts > All Hosts**。
7. 选择您要添加策略的主机或主机。
8. 点 **Select Action**。
9. 从列表中选择 **Assign Compliance Policy**。
10. 在 **Policy** 窗口中，从可用策略列表中选择您要的策略并点击 **Submit**。

7.7. 监控合规性

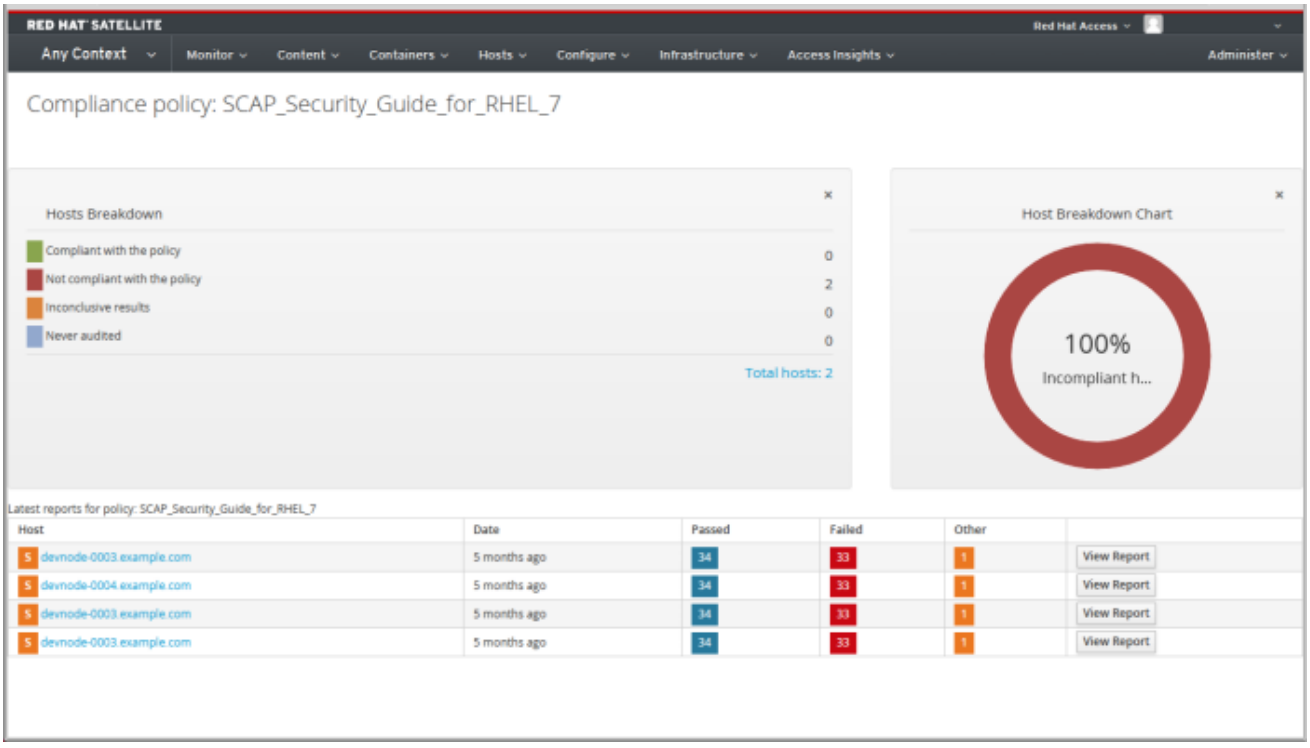
红帽卫星 6 支持集中合规性监控和管理。合规性仪表板提供了主机的合规性概述，以及在该策略范围内查看每个主机的详细信息。合规性报告提供有关使用适用策略每个主机的合规性的详细分析。通过这些信息，您可以评估每个主机呈现的风险，并管理使主机符合要求的资源。

使用 SCAP 监控合规性时的常见目标包括：

- 验证策略合规性。
- 检测合规性的变化。

7.7.1. 合规策略仪表板

合规性策略控制面板提供主机合规性的统计摘要，以及在该策略范围内查看每个主机的详细信息。对于被评估为不合规的所有主机，**Failed** 统计为优先合规工作提供了有用的指标。被检测到为 **Never audited** 的主机也应该是优先级，因为它们的状态未知。



7.7.2. 查看 Compliance Policy Dashboard

使用卫星 Web UI 验证策略与合规性策略仪表板的合规性。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Policies。
2. 点所需的策略名称。仪表板提供以下信息：
   - 演示了使用该策略主机合规的高级环图。
   - 统计分类，以表格格式使用策略合规主机。
   - 每个主机的最新策略报告链接。

7.7.3. 合规电子邮件通知

Satellite 服务器向订阅 Openscap 策略概述电子邮件通知的所有用户发送 OpenSCAP Summary 电子邮件。有关订阅电子邮件通知的详情请参考 第 6 章 配置电子邮件通知。每次运行策略时，卫星会根据之前运行检查结果，注意它们之间的任何更改。该电子邮件根据每个订阅者请求的频率发送，提供每个策略及其最新结果的摘要。

OpenSCAP Summary 电子邮件信息包含以下信息：

- 它涵盖的时间周期的详细信息。
- 状态中的所有主机总数：更改、合规和不合规。
- 每个主机的表格细分和最新策略的结果，包括通过、失败、更改或结果未知的规则总数。

7.7.4. 合规性报告

合规性报告是针对某一主机运行的策略的输出。每个报告包括每个策略通过或失败的规则总数。报告默认以降序列出。

在 Satellite Web UI 中，导航到 Hosts > Reports 以列出所有合规性报告。

合规性报告由以下区域组成：

- 简介
- 评估特性
- 合规性和评分
- 规则概述

评估特性

评估特性区域提供了针对特定配置集评估的详细信息，包括评估主机、评估中使用的配置集以及评估启动和完成评估时间。另外还会列出主机的 IPv4、IPv6 和 MAC 地址。

名称	描述	示例
目标机器	所评估主机的完全限定域名(FQDN)。	**test-system.example.com**
基准 URL	对主机被评估的 SCAP 内容的 URL。	**/var/lib/openscap/content/1fbdc87d24db51ca184419a2b6f**

名称	描述	示例
基准 ID	评估主机所针对的基准的标识符。基准是一组配置集	**xccdf_org.ssgproject.content_benchmark_RHEL_7**
配置文件 ID	评估主机所针对的配置集标识符。	**xccdf_org.ssgproject_content_profile_rht-ccp**
开始于	开始评估的日期和时间，采用 ISO 8601 格式。	**2015-09-12T14:40:02**
完成于	评估完成的日期和时间，格式为 ISO 8601。	**2015-09-12T14:40:05**
执行过程	在主机上执行评估的本地帐户名称。	**root**

合规性和评分

Compliance 和 Scoring 区域概述了主机是否合规规则、合规性故障按严重性划分，以及整体合规分数作为百分比。如果没有检查与规则的合规性，这将在 Rule results 字段中归类为其他 项。

规则概述

Rule Overview 区域提供有关每个规则和合规结果的详细信息，其规则以分级布局呈现。

选择或清除复选框，以缩小合规性报告中包含的规则列表。例如，如果您的审查的重点是任何不合规，请清除 pass 和 informational 复选框。

要搜索所有规则，在搜索字段中输入条件。搜索会根据您类型动态应用。Search 字段只接受单个纯文本搜索词，并以不区分大小写的搜索形式应用。当您执行搜索时，只会列出描述与搜索条件匹配的规则。要删除搜索过滤器，请删除搜索条件。

有关每个结果的说明，请将光标悬停在 Result 列中显示的状态。

7.7.5. 检查主机的合规性故障

使用卫星 Web UI 确定主机在规则中失败的原因。

流程

1. *在 Satellite Web UI 中，导航到 Hosts > Reports 以列出所有合规性报告。*
2. *单击特定主机行中的 View Report，以查看单个报告的详情。*
3. *点击规则的标题查看更多详情：*
   - *规则的描述，包含使主机符合条件的规则信息（如果可用）。*
   - *规则的比率。*
   - *在某些情况下，一个补救脚本。*

警告

不要实施任何推荐的补救操作或脚本，而无需在非生产环境中先测试它们。

7.7.6. 搜索合规性报告

使用 Compliance Reports 搜索字段，过滤任何给定主机子集的可用报告列表。

流程

- *要应用过滤器，请在搜索字段中输入搜索查询，然后点击 Search 。搜索查询不区分大小写。*

搜索用例

- *以下搜索查询会查找超过 5 个规则的所有合规性报告：*

  ```
  failed > 5
  ```

- *以下搜索查询查找在 1 月 1 日 YYYY 之后创建的所有合规性报告，适用于包含 prod- group 字符的主机：*

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

- *以下搜索查询从小时数中找到 rhel7_audit 合规性策略生成的所有报告：*

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

- *以下搜索查询会发现通过 XCCDF 规则的报告：*

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

- *以下搜索查询会发现失败的 XCCDF 规则：*

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

- *以下搜索查询会发现结果与失败或 XCCDF 规则不同：*

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

其它信息

- *要查看可用搜索参数的列表，请点击空 Search 字段。*

- 您可以针对以下逻辑运算符创建复杂的查询：和，而不是，具有。有关逻辑运算符的更多信息，请参阅 第 5.5.4 节 “Granular Search 支持的 Operator”。
- 您不能在搜索查询中使用正则表达式。但是，您可以在一个搜索表达式中使用多个字段。有关所有可用搜索 Operator 的更多信息，请参阅 第 5.5.4 节 “Granular Search 支持的 Operator”。
- 您可以为搜索添加书签以重复使用相同的搜索查询。更多信息请参阅 第 16.3.1 节 “创建书签”。

7.7.7. 删除合规性报告

要删除合规性报告，请完成以下步骤：

1. 在 Satellite Web UI 中，导航到 Hosts > Reports。
2. 在 Compliance Reports 窗口中，标识要删除的策略，并在策略名称右侧的右侧选择 Delete。
3. 点击 OK。

7.7.8. 删除多个合规性报告

您可以同时删除多个合规策略。但是，在卫星 Web UI 中，合规策略会被分页，因此您必须一次删除一个报告页面。如果要删除所有 OpenSCAP 报告，请使用 红帽卫星 API 指南的" 删除 OpenSCAP 报告" 部分中的脚本。

1. 在 Satellite Web UI 中，导航到 Hosts > Reports。
2. 在 Compliance Reports 窗口中，选择您要删除的合规性报告。
3. 在列表右上角，选择 Delete Reports。
4. 对要删除的多页重复这些步骤。

7.8. OPENSCAP 支持的规格

OpenSCAP 支持以下规格：

标题	描述	版本
XCCDF	可扩展配置清单描述格式	1.2
OVAL	开放漏洞和评估语言	5.11
-	资产识别	1.1
ARF	资产报告格式	1.1
CCE	常见配置枚举	5.0
CPE	常见平台枚举	2.3
CVE	常见的漏洞和风险	-

标题	描述	版本
CVSS	通用漏洞评分系统	2.0

第 8 章 备份 SATELLITE 服务器和胶囊服务器

您可以备份 Satellite 部署，以确保出现灾难时的 Red Hat Satellite 部署和相关数据的连续性。如果您的部署使用自定义配置，在规划备份和恢复策略时，您必须考虑如何处理这些自定义配置。

要创建 Satellite 服务器或胶囊服务器以及所有相关数据的备份，请使用 **satellite-maintain backup** 命令。强烈建议您在单独的系统中备份到单独的存储设备。

卫星服务在备份期间不可用。因此，您必须确保其他任务没有被其他管理员调度。您可以使用 **cron** 计划备份。如需更多信息，请参阅 第 8.5 节 "Weekly Full Backup Followed by Daily Incremental Backups 示例"。

在离线或快照备份过程中，服务处于不活跃状态，Satellite 处于维护模式。防火墙拒绝来自端口 443 之外的所有流量，以确保没有触发任何修改。

备份包含来自 **/root/ssl-build** 目录的敏感信息。例如，它可以包含主机名、ssh 密钥、请求文件和 SSL 证书。您必须加密或将备份移到安全位置，以便最大程度降低对主机的损坏或未授权访问的风险。

传统备份方法

您还可以使用传统的备份方法。如需更多信息，请参阅 Red Hat Enterprise Linux 7 系统管理员指南中的系统 备份和恢复。

注意

如果您计划使用 **satellite-maintain** 备份命令来 创建备份，请不要停止 **satellite-maintain** 服务。

- 在创建快照或传统备份时，您必须按如下方式停止所有服务：

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

- 在创建快照或传统备份后启动服务：

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

8.1. 估算备份的大小

完整备份可为 PostgreSQL 和 Pulp 数据库文件创建未压缩存档，以及卫星配置文件。创建存档后压缩发生，以减少 Satellite 服务不可用的时间。

完整备份需要空间来存储以下数据：

- 解压缩 Satellite 数据库和配置文件
- 压缩的 Satellite 数据库和配置文件
- 共有 20% 的存储空间，以确保备份可靠

流程

1. 输入 **du** 命令，以估算包含 Satellite 数据库和配置文件的未压缩目录大小：

```
# du -sh /var/opt/rh/rh-postgresql12/lib/pgsql/data /var/lib/pulp
```

```
100G  /var/opt/rh/rh-postgresql12/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. 计算存储压缩数据所需的空间量。
下表描述了备份中包含的所有数据项目的压缩率：

表 8.1. 备份数据压缩率

数据类型	目录	比率	结果示例
PostgreSQL 数据库文件	**/var/opt/rh/rh-postgresql12/lib/pgsql/data**	80 - 85%	100 GB → 20 GB
Pulp RPM 文件	**/var/lib/pulp**	（未压缩）	100 GB
配置文件	**/var/lib/qpidd** **/var/lib/tftpboot** **/etc** **/root/ssl-build** **/var/www/html/pub** **/opt/puppetlabs**	85%	942 MB → 141 MB

在本例中，压缩的备份数据总数为 180 GB。

3. 要计算需要存储备份的可用空间量，请计算压缩和未压缩备份数据估计值的总和，再添加额外的 20% 以确保备份可靠。
这个示例需要 681 GB，以及 180 GB 用于未压缩备份数据，总计 861 GB。使用 172 GB 的额外空间，必须为备份位置分配 1033 GB。

8.2. 执行 SATELLITE 服务器或 CAPSULE SERVER 的完整备份

Red Hat Satellite 6.10 使用 **satellite-maintain** 备份 命令进行备份。

备份卫星服务器的方法有三种：

- 离线备份
- 在线备份
- 快照备份
有关以上方法的更多信息，您可以查看每个备份方法的使用声明。

对于离线备份：

```
# satellite-maintain backup offline --help
```

进行在线备份：

```
# satellite-maintain backup online --help
```

对于快照备份：

```
# satellite-maintain backup snapshot --help
```

目录创建

satellite-maintain 备份 命令会在您指定的备份目录中创建一个时间戳的子目录。**satellite-maintain** 备份命令不会覆盖备份，因此您必须在从备份或增量备份中恢复时选择正确的目录或子目录。根据需要，**satellite-maintain backup** 命令停止并重启服务。

当您运行 **satellite-maintain** 备份离线 命令时，会创建以下默认备份目录：

- Satellite 上的 Satellite **-backup**
- Capsule 上的 **Foreman-proxy-backup**

如果要设置自定义目录名称，请添加 **--preserve-directory** 选项并添加目录名称。然后，备份将保存在您在命令行中提供的目录中。如果您使用 **--preserve-directory** 选项，如果备份失败，则不会删除数据。

请注意，如果您使用本地 PgSQL 数据库，则 **postgres** 用户需要对备份目录的写入权限。

远程数据库

您可以使用 **satellite-maintain backup** 命令备份远程数据库。

您可以使用在线和离线方法备份远程数据库，但如果您使用离线方法，如快照，**satellite-maintain** 备份命令执行数据库转储。

先决条件

- 确保您的备份位置有足够的磁盘空间来存储备份。更多信息请参阅 第 8.1 节 “估算备份的大小”。

流程

要对 Satellite 服务器或胶囊服务器执行完全离线备份，请完成以下步骤之一：

警告

请求卫星服务器或胶囊服务器的其他用户来保存任何更改，并提醒他们在备份期间没有 Satellite 服务。确保没有计划其他任务与备份相同的时间。

- 在 Satellite 服务器中输入以下命令：

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

- 在 Capsule Server 上，输入以下命令：

```
# satellite-maintain backup offline /var/foreman-proxy-backup
```

8.3. 执行没有 PULP 内容的备份

您可以执行排除 Pulp 目录的内容的离线备份。没有 Pulp 内容的备份对于调试用途很有用，仅用于在不备份 Pulp 数据库的情况下提供对配置文件的访问。您无法从不包含 Pulp 内容的目录中恢复。

警告

请求卫星服务器或胶囊服务器的其他用户来保存任何更改，并提醒他们在备份期间没有 Satellite 服务。确保没有计划其他任务与备份相同的时间。

先决条件

- 确保您的备份位置有足够的磁盘空间来存储备份。更多信息请参阅 第 8.1 节 “估算备份的大小”。

流程

- 要在没有 Pulp 内容的情况下执行离线备份，请输入以下命令：

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

8.4. 执行增量备份

使用这个步骤对自上次备份后的任何更改进行离线备份。

要执行增量备份，您必须执行完整备份作为创建序列的第一个增量备份的引用。保留最新的完整备份以及从中恢复的完整增量备份序列。

警告

请求卫星服务器或胶囊服务器的其他用户来保存任何更改，并提醒他们在备份期间没有 Satellite 服务。确保没有计划其他任务与备份相同的时间。

先决条件

- 确保您的备份位置有足够的磁盘空间来存储备份。更多信息请参阅 第 8.1 节 “估算备份的大小”。

流程

1. 要执行完全离线备份，请输入以下命令：

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

2. 要在备份目录中创建一个目录来存储第一个增量备份，请使用 **--incremental** 选项输入 **satellite-maintain backup** 命令：

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

3. 要创建第二个增量备份，使用 **--incremental** 选项输入 **satellite-maintain backup** 命令，并包含到第一个增量备份的路径，以指示下一增量备份的起点。这会在备份目录中为第二个增量备份创建一个目录：

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

4. 可选：如果要指向不同版本的备份，并使用该备份版本作为起始点进行一系列增量，则可以随时执行此操作。例如，如果要从完整备份而不是第一个增量备份中进行新的增量备份，请指向完整备份目录：

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

8.5. WEEKLY FULL BACKUP FOLLOWED BY DAILY INCREMENTAL BACKUPS 示例

以下脚本会在星期日执行完整备份，后接以下每个天的增量备份。针对执行增量备份的每天创建一个新子目录。该脚本需要每日 cron 作业。

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

请注意，**satellite-maintain backup** 命令要求 **/sbin** 和 **/usr/sbin** 目录位于 **PATH** 中，而 **--assumeyes** 选项则用于跳过确认提示。

8.6. 执行在线备份

仅针对调试目的执行在线备份。

与在线备份相关的风险

在执行在线备份时，如果存在影响 Pulp 数据库的步骤，则恢复的 Pulp 部分会重复，直到不再更改为止。因为 Pulp 数据库备份是备份 Satellite 的最耗时，因此如果更改了更改了 Pulp 数据库，则备份过程会保持重启。

对于生产环境，请使用快照方法。更多信息请参阅 第 8.7 节 “执行快照备份”。如果要在生产环境中使用在线备份方法，请谨慎操作，并确保备份过程中不会做任何修改。

警告

请求卫星服务器或胶囊服务器的其他用户来保存任何更改，并提醒他们在备份期间没有 Satellite 服务。确保没有计划其他任务与备份相同的时间。

先决条件

- 确保您的备份位置有足够的磁盘空间来存储备份。更多信息请参阅 第 8.1 节 “估算备份的大小”。

流程

- 要执行在线备份，请输入以下命令：

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

8.7. 执行快照备份

可以执行使用 Pulp 和 PostgreSQL 目录的逻辑卷管理器(LVM)快照的快照备份。从 LVM 快照创建备份可缓解不一致备份的风险。

快照备份方法比完全离线备份更快，因此减少了 Satellite 停机时间。

要查看 usage 语句，请输入以下命令：

```
satellite-maintain backup snapshot -h
```

警告

请求其他卫星服务器或胶囊服务器用户来保存任何更改，并提醒他们在备份期间没有 Satellite 服务。确保没有计划其他任务与备份相同的时间。

先决条件

在执行快照备份前，请确定满足以下条件：

- 系统将 LVM 用于您快照的目录：**/var/lib/pulp/** 和 **/var/opt/rh-postgresql12/lib/pgsql**。
- 相关卷组(VG)中的可用磁盘空间是快照大小三倍。更加精确，VG 必须为成员逻辑卷(LV)有足够的空间 **unreserved**，以适应新快照。另外，一个 LV 必须有足够的可用空间用于备份目录。
- 目标备份目录位于与您快照的目录不同的 LV 上。

流程

- 要执行快照备份，请输入 **satellite-maintain** 备份快照 命令：

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

satellite-maintain backup snapshot 命令在服务处于活跃状态时创建快照，并停止所有可能会影响备份的服务。这样可以缩短维护窗口。成功快照后，所有服务都会重启，并删除 LVM 快照。

8.8. 在执行备份时列出和跳过步骤

使用 **satellite-maintain** 备份 命令进行一系列步骤的备份。要跳过备份部分将 **--whitelist** 选项添加到命令中，并添加您要省略的 step 标签。

- 要显示可用步骤标签列表，请输入以下命令：

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

- 要跳过备份步骤，请使用 **--whitelist** 选项输入 **satellite-maintain backup** 命令。例如：

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

第 9 章 从备份中恢复 SATELLITE 服务器或胶囊服务器

您可以从作为 第 8 章 备份 Satellite 服务器和胶囊服务器 的一部分创建的备份数据恢复 Red Hat Satellite 服务器或红帽 Capsule Server。这个过程概述了如何在生成备份的同一服务器上恢复备份，并在目标系统上删除备份涵盖的所有数据。如果原始系统不可用，请置备具有相同配置设置和主机名的系统。

9.1. 从完整备份中恢复

使用这个流程从完整备份中恢复 Red Hat Satellite 或 Capsule Server。恢复过程完成后，所有进程都在线，所有数据库和系统配置都会恢复到备份时的状态。

先决条件

- 确保您要恢复到正确的实例。Red Hat Satellite 实例必须具有与原始系统相同的主机名、配置和相同次要版本(X.Y)。
- 请确定您已有的目标目录。目标目录是从存档中包含的配置文件读取的。
- 确保有足够的空间将这些数据存储在卫星服务器或胶囊服务器的基本系统中，以及在恢复包含备份中的 /etc/ 和 /var/ 目录中的所有 数据后有足够的空间。
  要检查目录所使用的空间，请输入以下命令：

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

  要检查可用空间，请输入以下命令：

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

  添加 **--total** 选项，从多个目录中获得结果总数。
- 确保所有 SELinux 上下文都正确。输入以下命令恢复正确的 SELinux 上下文：

  ```
  # restorecon -Rv /
  ```

流程

1. 选择安装 Satellite 或 Capsule 的适当方法：
   - 要从连接的网络安装卫星服务器，请按照从连接的网络安装卫星服务器中的步骤操作。https://access.redhat.com/documentation/zh-cn/red_hat_satellite/6.10/html-single/installing_satellite_server_from_a_connected_network/index#
   - 要从断开连接的网络中安装 Satellite Server，请按照 从断开连接的网络安装 Satellite Server 中的步骤操作。
   - 要安装胶囊服务器，请按照 安装胶囊服务器 中的步骤操作。
2. 将备份数据复制到卫星服务器的本地文件系统。使用 /var/ 或 /var/tmp/。
3. 运行恢复脚本。

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

   其中 backup_directory 是时间戳目录或包含备份数据的子目录。

恢复过程可能需要很长时间才能完成，因为要复制的数据量。

其它资源

- 要进行故障排除，您可以检查 **/var/log/foreman/production.log** 和 **/var/log/messages**。

9.2. 从增量备份中恢复

使用这个流程从增量备份中恢复 Satellite 或胶囊服务器。如果您有多个增量备份分支，请根据需要按时间顺序为"branch"选择每个增量备份。

恢复过程完成后，所有进程都在线，所有数据库和系统配置都会恢复到备份时的状态。

流程

1. 使用 第 9.1 节 “从完整备份中恢复” 中的说明恢复最后的完整备份。
2. 从 Satellite 服务器的本地文件系统中删除完整备份数据，例如 **/var/** 或 **/var/tmp/**。
3. 将增量备份数据复制到卫星服务器的本地文件系统，例如 **/var/** 或 **/var/tmp/**。
4. 在相同序列中恢复增量备份：

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

如果您使用 **satellite-maintain backup** 命令创建备份，则不需要在 命令中使用 **-i** 选项。

其它资源

- 要进行故障排除，您可以检查 **/var/log/foreman/production.log** 和 **/var/log/messages**。

9.3. 使用虚拟机快照备份和恢复胶囊服务器

如果您的胶囊服务器是一个虚拟机，您可以从快照中恢复。建议创建用于恢复的每周快照。在发生故障时，您可以安装或配置新的胶囊服务器，然后从卫星服务器同步数据库内容。

如果需要，部署新的胶囊服务器，确保主机名与之前相同，然后安装胶囊证书。您仍然可以在卫星服务器上，软件包名称以 **-certs.tar** 结束，或者创建新服务器。按照 安装胶囊服务器中的步骤进行操作，直到您可以在 Web UI 中确认该胶囊服务器。然后使用流程 第 9.3.1 节 “同步外部胶囊” 从 Satellite 同步。

9.3.1. 同步外部胶囊

将外部胶囊与卫星同步。

流程

1. 要同步外部胶囊，请在 Web UI 中选择相关组织和位置，或者选择 Any Organization 和 Any Location。
2. 导航到 Infrastructure > Capsules，再单击要同步的 Capsule 的名称。
3. 在 Overview 选项卡中，选择 Synchronize。

第 10 章 重命名 SATELLITE SERVER 或 CAPSULE SERVER

若要重命名卫星服务器或胶囊服务器，您必须使用 **satellite-change-hostname** 脚本。

如果重命名了卫星服务器，您必须重新注册所有 Satellite 客户端，并将每个胶囊服务器配置为指向新的 Satellite 主机名。如果您使用自定义 SSL 证书，则必须使用新主机名重新生成它们。如果使用 virt-who，您必须更新具有新主机名的 virt-who 配置文件。

如果重命名了胶囊服务器，您必须重新注册所有胶囊客户端，并在卫星 Web UI 中更新胶囊主机名。如果您使用自定义 SSL 证书，则必须使用新主机名重新生成它们。

警告

重命名过程将关闭要重命名的主机上的所有卫星服务器服务。重命名完成后，所有服务都会重启。

10.1. 重命名卫星服务器

卫星服务器的主机名供卫星服务器组件、所有胶囊服务器以及注册给它通信的主机使用。此流程确保您更新新主机名的所有引用。

如果使用外部身份验证，您必须在运行 **satellite-change-hostname** 脚本后重新配置卫星服务器以进行外部身份验证。**satellite-change-hostname** 脚本会破坏卫星服务器的外部身份验证。有关配置外部验证的详情，请参考 第 13 章 配置外部身份验证。

如果使用 virt-who，您必须在运行 **satellite-change-hostname** 脚本后更新带有新主机名的 virt-who 配置文件。如需更多信息，请参阅在 Red Hat Satellite 中配置虚拟机订阅中的修改 virt-who 配置。

先决条件

- **hostname** 和 **hostname -f** 命令必须返回 Satellite Server 的 FQDN 或 **satellite-change-hostname** 脚本将无法完成。如果 **hostname** 命令返回 Satellite Server 的短名称，则使用 **hostnamectl set-hostname old_fqdn** 在尝试使用 **satellite-change-hostname** 脚本前正确设置旧 FQDN。
- 在更改主机名前，执行卫星服务器的备份。如果重命名过程不成功，您必须从备份中恢复它。更多信息请参阅 第 8 章 备份 Satellite 服务器和胶囊服务器。
- 可选：如果卫星服务器安装了自定义 SSL 证书，则必须为主机的新名称获取新证书。如需更多信息，请参阅 从连接的网络安装卫星服务器中的使用自定义 SSL 证书配置 Satellite 服务器。

流程

1. 在卫星服务器上，选择运行 **satellite-change-hostname** 脚本的适当方法，提供新的主机名和 Satellite 凭证：
   - 如果您的 Satellite 服务器安装有默认自签名 SSL 证书，请输入以下命令：

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

- 如果您的 Satellite 服务器使用自定义 SSL 证书安装：

```
# satellite-change-hostname new-satellite \
--username admin \
--password password \
--custom-cert "/root/owncа/test.com/test.com.crt" \
--custom-key "/root/owncа/test.com/test.com.key"
```

2. 可选：如果您为新的 Satellite 服务器主机名创建了自定义 SSL 证书，请运行 Satellite 安装脚本来安装证书。有关安装自定义 SSL 证书的更多信息，请参阅 从连接的网络安装卫星服务器中的部署自定义 SSL 证书 到卫星服务器。

3. 在所有 Satellite 客户端上，输入以下命令重新安装 bootstrap RPM、重新注册客户端并刷新其订阅。
您可以使用远程执行功能来执行此步骤。如需更多信息，请参阅 管理主机中的配置和设置远程作业 。

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

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

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

# subscription-manager refresh
```

4. 在所有胶囊服务器中，运行 Satellite 安装脚本来更新对新主机名的引用：

```
# satellite-installer \
--foreman-proxy-foreman-base-url https://new-satellite.example.com \
--foreman-proxy-trusted-hosts new-satellite.example.com \
--puppet-server-foreman-url new-satellite.example.com
```

5. 在卫星服务器上，列出所有胶囊服务器：

```
# hammer capsule list
```

6. 在卫星服务器上，同步每个胶囊服务器的内容：

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

10.2. 重命名胶囊服务器

胶囊服务器的主机名由卫星服务器组件引用，并且注册了所有主机。此流程确保您更新新主机名的所有引用。

注意

- **hostname** 和 **hostname -f** 命令必须返回 Capsule Server 的 FQDN 或 **satellite-change-hostname** 脚本将无法完成。
- 如果 **hostname** 命令返回 Capsule Server 的短名称，则使用 **hostnamectl set-hostname old_fqdn** 在尝试使用 **satellite-change-hostname** 脚本前正确设置旧 FQDN。

先决条件

- 备份胶囊服务器。**satellite-change-hostname** 脚本对胶囊服务器进行不必要的更改。如果重命名过程不成功，您必须从备份中恢复它。
  在更改主机名前执行备份。更多信息请参阅 第 8 章 备份 Satellite 服务器和胶囊服务器。

警告

在 BZ#1829115 被解决前，您必须编辑 Capsule 服务器上的 **usr/share/katello/hostname-change.rb** 文件，并在尝试重命名胶囊服务器前注释掉以下行：

```
STDOUT.puts "updating hostname in hammer configuration"
self.run_cmd("sed -i.bak -e 's/#{@old_hostname} \
/#{@new_hostname}/g' #{hammer_root_config_path}/*.yml")
self.run_cmd("sed -i.bak -e 's/#{@old_hostname} \
/#{@new_hostname>/g' #{hammer_config_path}/*.yml")
```

流程

1. 在卫星服务器上，为胶囊服务器生成一个新的证书存档文件。
   - 如果您使用默认 SSL 证书，请输入以下命令：

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

     请确定您输入到 **.tar** 文件的完整路径。
   - 如果您使用自定义 SSL 证书，请为胶囊服务器创建一个新的 SSL 证书。如需更多信息，请参阅安装胶囊服务器中的使用自定义 SSL 证书配置胶囊服务器。
2. 在卫星服务器上，将证书存档文件复制到胶囊服务器，并在提示时提供 **root** 用户密码。在本例中，存档文件被复制到 **root** 用户的主目录中，但您最好将其复制到其他位置。

   ```
   # scp /root/new-capsule.example.com-certs.tar root@capsule.example.com:
   ```
3. 在 Capsule Server 上，运行 **satellite-change-hostname** 脚本，并提供主机的新名称、卫星凭据和证书存档文件名。

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

请确定您输入到 **.tar** 文件的完整路径。

4. 可选：如果您为胶囊服务器创建了自定义证书，则在胶囊服务器上部署证书，请输入 **Capsule-certs-generate** 命令返回的 **satellite- installer** 命令。如需更多信息，请参阅安装胶囊服务器中的 部署自定义 SSL 证书到胶囊服务器。

5. 在所有胶囊客户端上，输入以下命令重新安装 **bootstrap RPM**、重新注册客户端并刷新其订阅。您可以使用远程执行功能来执行此步骤。如需更多信息，请参阅 管理主机中的配置和设置远程作业。

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

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

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

# subscription-manager refresh
```

6. 在 **Satellite Web UI** 中，导航到 **Infrastructure > Capsules**。

7. 在列表中找到胶囊服务器，再单击它右侧的 **Edit**。

8. 编辑 **Name** 和 **URL** 字段，以匹配胶囊服务器的新主机名，然后单击 **Submit**。

9. 在您的 **DNS** 服务器上，为胶囊服务器的新主机名添加一个记录，并删除上一主机名的记录。

第 11 章 维护 SATELLITE 服务器

本章介绍了如何维护红帽卫星服务器的信息，包括有关如何使用审计记录的信息、如何清理未使用的任务以及如何从完整磁盘中恢复 Pulp。

11.1. 删除审计记录

在 Satellite 中自动创建审计记录。您可以使用 **foreman-rake audits:expire** 命令随时删除审计。您还可以使用 cron 作业以设定的时间间隔来调度审计记录删除。

默认情况下，使用 **foreman-rake audits:expire** 命令删除超过 90 天的审计记录。您可以通过添加 **days** 选项并添加天数来指定保留审计记录的天数。

例如，如果您想要删除超过七天的审计记录，请输入以下命令：

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

11.2. 匿名审计记录

您可以使用 **foreman-rake audits:anonymize** 命令删除任何用户帐户或 IP 信息，同时维护数据库中的审计记录。您还可以使用 cron 作业按您想要设定的间隔调度审计记录。

默认情况下，使用 **foreman-rake audits:anonymize** 命令 aonymizes audit 记录，超过 90 天。您可以通过添加 **days** 选项并添加天数来指定保留审计记录的天数。

例如，如果要匿名化超过七天的审计记录，请输入以下命令：

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

11.3. 配置 CLEANING UNUSED TASKS 功能

卫星定期执行清理以减少数据库中的磁盘空间，并限制磁盘增长速度。因此，卫星备份可以更快地完成，并且整体性能更高。

默认情况下，卫星执行 cron 作业，该作业每天在 19:45 处清理任务。Satellite 在清理过程中删除以下任务：

- 运行成功并超过三十天的任务
- 所有超过一年的任务

对于 Satellite 从之前版本升级

在 BZ#1788615 解决前，这个功能仅适用于 Satellite 6.10 及更新版本的全新安装。如果您从之前的版本升级 Satellite，则这个功能会被默认禁用。要启用 Satellite 执行常规清理，请输入以下命令：

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

（可选）使用此流程调整配置以满足您的需要。

流程

1. 可选：要配置 Satellite 运行 cron 作业的时间，请将 **--foreman-plugin-tasks-cron-line** 参数设置为您需要以 cron 格式运行的时间。例如，要将 cron 任务调度到每天 15:00 运行，请输入以下命令：

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

2. 可选：要配置 Satellite 删除任务的周期，请编辑 **/etc/foreman/plugins/foreman-tasks.yaml** 文件中的 **:rules:** 部分。

11.4. 从完整磁盘中恢复

下面的步骤描述了如何在逻辑卷(LV)中使用 Pulp 数据库没有可用空间时解决这种情况。

从完整磁盘中恢复

1. 让运行 Pulp 任务完成，但不会触发任何新任务，因为它们可能会因为完整磁盘而失败。
2. 确定具有 **/var/lib/pulp** 目录的 LV 具有足够的空闲空间。以下是实现这一点的方法：
   a. 删除孤立的内容：

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

   这会每周运行，以便它不会释放更多空间。

   b. 将下载策略从 Immediate 改为 On Demand，以便尽可能多的软件仓库并删除已下载的软件包。具体步骤请查看红帽知识库解决方案 如何将 Satellite 上存储库的同步策略从 "Immediate" 改为 "On-Demand "。

   c. 使用 **/var/lib/pulp** 目录在 LV 上增大文件系统。如需更多信息，请参阅 Red Hat Enterprise Linux 7 Logical Volume Administration Guide 中的逻辑卷中增大文件系统。

注意

如果您使用不确定的文件系统（例如 ext3、ext4 或 xfs），您可能需要卸载该文件系统，使其不会被使用。在这种情况下，请完成以下步骤：

1. 停止 **satellite-maintain** 服务：

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

2. 在 LV 上增加文件系统。
3. 启动 **satellite-maintain** 服务：

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

3. 如果由于完整磁盘导致一些 Pulp 任务失败，请再次运行它们。

11.5. 在 SATELLITE 或 CAPSULE 的基本操作系统上管理软件包

要在 Satellite 或 Capsule 基础操作系统中安装和更新软件包，您必须输入 **satellite-maintain packages** 命令。

Satellite 可防止用户使用 yum 安装和更新软件包，因为 **yum** 也可能会更新与 Satellite 或 Capsule 相关的软件包，并导致系统不一致。

重要

satellite-maintain packages *命令在运行它的操作系统中重新启动一些服务，因为它在安装软件包后运行* ***satellite-installer*** *命令。*

流程

- *要在 Satellite 或 Capsule 上安装软件包，请输入以下命令：*

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

- *要在 Satellite 或 Capsule 上更新特定软件包，请输入以下命令：*

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

- *要更新 Satellite 或 Capsule 中的所有软件包，请输入以下命令：*

```
# satellite-maintain packages update
```

使用 yum 检查软件包更新

*如果要使用 **yum** 检查更新，请输入命令手动安装和更新软件包，然后使用 **yum** 检查更新：*

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

单独更新软件包可能会导致 Satellite 或 Capsule 中的软件包不一致。有关更新 Satellite 中软件包的更多信息，请参阅更新卫星服务器。

为 Satellite 或 Capsule Package Management 启用 yum

*如果您要直接使用 **yum** 直接安装和更新软件包，并自行控制系统稳定性，请输入以下命令：*

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

将软件包管理恢复到默认设置

*如果要恢复默认设置并启用 Satellite 或 Capsule，以防止用户使用 **yum** 安装和更新软件包，并确保系统的稳定性，请输入以下命令：*

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

11.6. 重新声明 POSTGRESQL 空间

PostgreSQL 数据库可以使用大量磁盘空间，特别是载入的部署中。使用此流程在 Satellite 上重新声明一些磁盘空间。

流程

1. *停止除* ***postgresql*** *服务外的所有服务：*

```
# satellite-maintain service stop --exclude postgresql
```

2. *切换到* ***postgres*** *用户并重新声明数据库中的空间：*

```
# su - postgres -c 'vacuumdb --full --dbname=foreman'
```

3. ***vacuum*** *完成后启动其他服务：*

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

4. *确认* ***/var/lib/pgsql/*** *目录中存在这些文件：*

```
# ls -l /var/lib/pgsql/

# du -sh /var/lib/pgsql/
```

5. *从* ***/var/lib/pgsql/*** *目录中删除数据：*

```
# rm -rf /var/lib/pgsql/*
```

第 12 章 日志记录和报告问题

本章提供了有关如何在 Red Hat Satellite 服务器中记录和报告问题的信息，包括相关日志文件的信息、如何启用调试日志记录、创建支持问题单并附加相关的日志 tar 文件，以及如何在 Satellite Web UI 中访问支持问题单。

您可以使用本章中描述的日志文件和其他信息进行自己的故障排除，或者您可以捕获这些文件和更多文件，以及诊断和配置信息，以发送给红帽支持。

有关 Satellite 日志记录设置的更多信息，请使用 **satellite-installer** 和 **--full-help** 选项：

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

12.1. 启用调试日志记录

调试日志记录提供最详细的日志信息，有助于对 Satellite 6.10 及其组件可能出现的问题进行故障排除。

在 Satellite CLI 中，启用 debug 日志记录来记录 Satellite 6.10 的详细信息。

流程

要启用调试日志记录，请在卫星服务器上完成以下步骤。

1. 要启用调试日志记录，请输入以下命令：

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

2. 完成调试后，将日志级别重置为默认值：

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

12.2. 启用单个日志记录器

您可以为选择性日志记录启用单独的日志记录器。Satellite 使用以下日志记录器：

app
: 记录 Web 请求和所有常规应用消息。默认值：true。

audit
: 记录其他事实统计、添加、更新和删除事实的数量。默认值：true。

ldap
: 记录高级 LDAP 查询和 LDAP 操作。默认值：false。

权限
: 在加载页面时，记录用户角色、过滤器和权限的查询。默认值：false。

sql
: 通过 Rails ActiveRecord 发出的 SQL 查询日志。默认值：false。

流程

要启用单个日志记录器，请完成以下步骤。

1. 启用您想要的独立日志记录器。例如，要启用 **sql** 和 **ldap** loggers，请输入以下命令：

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

2. 可选：要将日志记录器重置为默认值，请输入以下命令：

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

12.3. 配置日志记录到日志

您可以配置 Satellite 以使用 Journal 管理日志。然后日志日志消息转发到 **rsyslog**，并且 **rsyslog** 会将日志消息写入 **/var/log/messages**。请注意，在更改日志消息后，日志消息不会显示在 **/var/log/foreman/production.log** 或 **/var/log/foreman-proxy.log** 中。

有关日志的更多信息，请参阅 **Red Hat Enterprise Linux 7** 系统管理员指南中的使用日志。

流程

要使用 Journal 配置 Satellite 服务器日志，请完成以下步骤：

1. 输入以下 **satellite-installer** 命令，将日志记录配置为 **journald** ：

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

2. 重启 Apache 守护进程：

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

12.4. SATELLITE 提供的日志文件目录

红帽卫星以通知和日志文件的形式提供系统信息。

表 12.1. 用于报告和故障排除的日志文件目录

日志文件目录	日志文件内容的描述
/var/log/candlepin	订阅管理
/var/log/foreman	Foreman
/var/log/foreman-proxy	Foreman 代理
/var/log/httpd	Apache HTTP 服务器
/var/log/foreman-installer	安装程序
/var/log/puppet	配置管理
/var/log/rhsm	订阅管理

日志文件目录	日志文件内容的描述
/var/log/tomcat	Candlepin webservice 日志
/var/log/messages	各种其他日志消息

*您还可以使用 **foreman-tail** 命令遵循与 Satellite 相关的许多日志文件。您可以运行**foreman-tail -l** 来列出其后面的进程和服务。*

12.5. COLLECTING 日志信息的工具

有两个实用程序可以从日志文件收集信息。

表 12.2. 日志收集工具

命令	描述
foreman-debug	**foreman-debug** 命令收集 Red Hat Satellite 的配置和日志文件数据、其后端服务和系统信息。该信息将收集并写入 tar 文件。默认情况下，输出 tar 文件位于 **/tmp/*foreman-debug-xxx.tar.xz***。 另外，**foreman-debug** 命令导出在最后 60 天中运行的任务。默认情况下，输出 tar 文件位于 **/tmp/*task-export-xxx.tar.xz***。如果缺少文件，请查看 **/tmp/task-export.log** 文件，以了解任务导出失败的原因。 如需更多信息，请运行 **foreman-debug --help**。 运行此命令时没有超时。
sosreport	**sosreport** 命令是一个从 Red Hat Enterprise Linux 系统收集配置和诊断信息的工具，如运行的内核版本、载入的模块和服务配置文件。该命令还运行外部程序（例如：**foreman-debug -g**）来收集 Satellite 特定信息，并将这一输出存储在 tar 文件中。 默认情况下，输出 tar 文件位于 **/var/tmp/*sosreport-XXX-20171002230919.tar.xz***。如需更多信息，请运行 **sosreport --help** 或查看 *sosreport 是什么以及如何创建*? **sosreport** 命令调用 **foreman-debug -g**，并在 500 秒后超时。如果您的 Satellite 服务器有大型日志文件或多个 Satellite 任务，在创建一个支持问题单时，支持工程师可能需要 **sosreport** 和 **foreman-debug** 的输出。

重要

***foreman-debug** 和**sosreport** 在收集信息的同时删除密码、令牌和密钥等安全信息。但是，**tar** 文件仍然可以包含有关红帽卫星服务器的敏感信息。红帽建议您将这些信息直接发送到预期的接收者而不是一个公共目标。*

第 13 章 配置外部身份验证

通过使用外部身份验证，您可以从外部身份提供程序中的用户组成员资格生成用户和用户组权限。使用外部身份验证时，您不必在卫星服务器上创建这些用户并手动维护其组成员资格。

重要用户和组群帐户信息

所有用户和组群帐户必须是本地帐户。这是为了确保卫星服务器上的本地帐户和 Active Directory 域中的帐户之间没有身份验证冲突。

如果您的 **/etc/passwd** 和 **/etc/group** 文件中存在用户和组群帐户，则您的系统不会受到这个冲突的影响。例如，要检查 **/etc/passwd** 和 **/etc/group** 文件中是否存在 **puppet**、**apache**、**foreman** 和 **foreman-proxy** 组的条目，请输入以下命令：

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

配置外部身份验证的情况

Red Hat Satellite 支持以下配置外部身份验证的一般场景：

- 使用 轻量级目录访问协议(LDAP)服务器作为外部身份提供程序。LDAP 是一组开放协议，用于通过网络访问集中存储的信息。使用 Satellite，您可以通过 Satellite Web UI 完全管理 LDAP。更多信息请参阅 第 13.1 节 “使用 LDAP”。虽然您可以使用 LDAP 连接到 Red Hat Identity Management 或 AD 服务器，但设置不支持服务器发现、跨林信任，或使用 Satellite Web UI 中的 Kerberos 进行单点登录。
- 将红帽身份管理服务器用作外部身份提供程序。红帽身份管理旨在管理个人身份、其在网络环境中使用的凭据和权限。无法使用红帽身份管理配置，只能使用卫星 Web UI 来完成，需要一些与 CLI 交互。更多信息请参阅 第 13.2 节 “使用 Red Hat Identity Management”。
- 使用与红帽身份管理集成的 Active Directory (AD)，将跨林 Kerberos 信任作为外部身份提供程序。更多信息请参阅 第 13.3.5 节 “带有 Cross-Forest Trust 的 Active Directory”。
- 使用红帽单点登录作为 OpenID 供应商，实现对 Satellite 的外部身份验证。更多信息请参阅 第 13.8 节 “使用 Red Hat Single Sign-On 身份验证配置 Satellite”。
- 使用 Red Hat Single Sign-On 作为 OpenID 供应商，使用 TOTP 向 Satellite 进行外部身份验证。更多信息请参阅 第 13.9 节 “使用 TOTP 配置红帽单点登录身份验证”。

此外，也提供对卫星服务器的访问权限，也可与红帽身份管理域集成。Red Hat Satellite 有一个 realm 功能，它可自动管理注册到某个域或域提供程序的任何系统的生命周期。更多信息请参阅 第 13.7 节 “Provisioned 主机的外部身份验证”。

表 13.1. 身份验证概述

类型	身份验证	用户组
Red Hat Identity Management	Kerberos 或 LDAP	是
Active Directory	Kerberos 或 LDAP	是
POSIX	LDAP	是

13.1. 使用 LDAP

卫星支持使用一个或多个 LDAP 目录进行 LDAP 身份验证。

如果您需要 Red Hat Satellite 使用 **TLS** 建立安全 LDAP 连接(LDAPS)，首先获取您要连接的 LDAP 服务器使用的证书，并将其标记为卫星服务器基本操作系统的信任，如下所述。如果您的 LDAP 服务器使用带有中间证书颁发机构的证书链，则链中所有根和中间证书都必须被信任，因此请确保获取所有证书。如果您此时不需要安全的 LDAP，请执行 第 13.1.2 节 "将 Red Hat Satellite 配置为使用 LDAP"。

使用 SSSD 配置

虽然本节中介绍了直接 LDAP 集成，红帽建议您使用 SSSD 并根据 Red Hat Identity Management、AD 或 LDAP 服务器进行配置。SSSD 提高了身份验证过程的一致性。有关首选配置的详情，请参考 第 13.3 节 "使用 Active Directory"。您还可以缓存 SSSD 凭证，并将其用于 LDAP 身份验证。有关 SSSD 的详情，请参考 Red Hat Enterprise Linux 7 System-Level 身份验证指南中的配置 SSSD。

13.1.1. 为 Secure LDAP 配置 TLS

使用 Satellite CLI 为安全 LDAP(LDAPS)配置 TLS。

流程

1. 从 LDAP 服务器获取证书。
   a. 如果您使用 Active Directory 证书服务，请使用 Base-64 编码的 X.509 格式导出企业 PKI CA 证书。如需有关 从 Active Directory 服务器创建和导出 CA 证书的信息，请参阅如何使用 Satellite 6 上的 TLS 配置 Active Directory 身份验证。
   b. 将 LDAP 服务器证书下载到安装卫星服务器的 Red Hat Enterprise Linux 系统上的临时位置，并在完成后将其移除。
   例如：**/tmp/example.crt**。文件名扩展 **.cer** 和 **.crt** 只包括惯例，可以引用 DER 二进制或 PEM ASCII 格式证书。
2. 信任 LDAP 服务器中的证书。
   Red Hat Satellite Server 需要 CA 证书使 LDAP 身份验证成为 **/etc/pki/tls/certs/** 目录中的单个文件。
   a. 使用 **install** 命令将导入的证书安装到具有正确权限的 **/etc/pki/tls/certs/** 目录中：

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

   b. 以 **root** 用户身份输入以下命令信任从 LDAP 服务器获得的**example.crt** 证书：

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

   c. 重启 **httpd** 服务：

```
# systemctl restart httpd
```

13.1.2. 将 Red Hat Satellite 配置为使用 LDAP

在卫星 Web UI 中，将 Satellite 配置为使用 LDAP。

请注意，如果您需要在 Satellite Web UI 中使用 Kerberos 的单点登录功能，您应该改为使用 Red Hat Identity Management 和 AD 外部身份验证。如需了解更多有关这些选项的信息，请参阅使用红帽身份管理 或使用Active Directory。

流程

1. 将 Network Information System(NIS)服务布尔值设置为 true，以防止 SELinux 停止传出 LDAP 连接：

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

2. 进入 Administer > LDAP Authentication。
3. 点 Create Authentication Source。
4. 在 LDAP 服务器 选项卡中，输入 LDAP 服务器的名称、主机名、端口和服务器类型。默认端口为 389，默认服务器类型是 POSIX（您可以原生选择 FreeIPA 或 Active Directory，具体取决于身份验证服务器类型）。对于 TLS 加密的连接，请选择LDAPS 复选框来启用加密。端口应更改为 636，这是 LDAPS 的默认设置。
5. 在 帐户 选项卡中，输入帐户信息和域名详情。有关描述和示例，请参阅 第 13.1.3 节 “LDAP 设置的描述”。
6. 在 Attribute mappings 选项卡上，将 LDAP 属性映射到 Satellite 属性。您可以映射登录名称、名字、姓氏、电子邮件地址和照片属性。如需示例，请参阅 第 13.1.4 节 “LDAP 连接的设置示例”。
7. 在位置 选项卡上，从左侧列表中选择位置。选择的位置分配给从 LDAP 身份验证源创建的用户，并在第一次登录时可用。
8. 在 Organizations 选项卡上，从左侧列表中选择机构。所选机构被分配给从 LDAP 身份验证源创建的用户，并在第一次登录时可用。
9. 点 Submit。
10. 为 LDAP 用户配置新帐户：
    - 如果您没有选择 Automatically Create Accounts In Satellite复选框，请参阅 第 5.1.1 节 “创建用户” 来手动创建用户帐户。
    - 如果您选择了 Automatically Create Accounts In Satellite复选框，LDAP 用户现在可以使用其 LDAP 帐户和密码登录到 Satellite。第一次登录后，Satellite 管理员必须手动为其分配角色。请参阅 第 5.1.2 节 “为用户分配角色” 在 Satellite 中分配适当的角色。

13.1.3. LDAP 设置的描述

下表提供了 帐户 选项卡中每个设置的描述。

表 13.2. 帐户标签设置

设置	描述

设置	描述
帐户	对 LDAP 服务器具有读访问权限的 LDAP 帐户的用户名。如果服务器允许匿名读取，则不需要用户名，否则使用用户对象的完整路径。例如： `uid=$login,cn=users,cn=accounts,dc=example,dc=com` **$login** 变量以字面字符串的形式存储在登录页面中输入的用户名。在扩展变量时，可以访问该值。 该变量无法从 LDAP 源与外部用户组一起使用，因为卫星需要在没有用户登录的情况下检索组列表。使用匿名或专用服务用户。
帐户密码	**帐户用户名** 字段中定义的用户的 LDAP 密码。如果**帐户用户名** 正在使用 **$login** 变量，则此字段可以保持空白。
基本 DN	LDAP 目录的顶级域名。
组基本 DN	包含组的 LDAP 目录树的顶级域名。
LDAP 过滤器	用于限制 LDAP 查询的过滤器。
自动创建帐户在 Satellite 中	如果选中此复选框，卫星在第一次登录 Satellite 时为 LDAP 用户创建用户帐户。第一次登录后，Satellite 管理员必须手动为其分配角色。请参阅 第 5.1.2 节 “为用户分配角色” 在 Satellite 中分配适当的角色。
Usergroup Sync	如果选择了此选项，用户组成员资格会在用户登录时自动同步，以确保成员资格始终保持最新状态。如果清除此选项，Satellite 依赖于 cron 作业来定期同步组成员资格（默认为 30 分钟）。更多上下文请查看 配置外部用户组：。

13.1.4. LDAP 连接的设置示例

*下表显示了不同类型的 **LDAP** 连接的设置示例。以下示例使用一个名为 **redhat** 的专用服务帐户，该帐户对用户和组条目具有绑定、读取和搜索权限。请注意，**LDAP** 属性名称区分大小写。*

表 13.3. Active Directory 的设置示例、可用 IPA 或红帽身份管理和 POSIX LDAP 连接

设置	Active Directory	FreeIPA 或红帽身份管理	POSIX (OpenLDAP)
帐户	DOMAIN\redhat	uid=redhat,cn=users, cn=accounts,dc=example, dc=com	uid=redhat,ou=users, dc=example,dc=com
帐户密码	P@ssword	-	-
基本 DN	DC=example,DC=COM	dc=example,dc=com	dc=example,dc=com
组基本 DN	CN=Users,DC=example,DC=com	cn=groups,cn=accounts, dc=example,dc=com	cn=employee,ou=userclass, dc=example,dc=com

设置	Active Directory	FreeIPA 或红帽身份管理	POSIX (OpenLDAP)
login name 属性	userPrincipalName	uid	uid
名字属性	givenName	givenName	givenName
姓氏属性	sn	sn	sn
电子邮件地址属性	mail	mail	mail
photo 属性	thumbnailPhoto	-	-

注意

***userPrincipalName** 允许在用户名中使用空格。登录名称属性 **sAMAccountName**（未列在上表中列出）提供了与传统的 **Microsoft** 系统的向后兼容性。**sAMAccountName** 不允许在用户名中使用空格。*

13.1.5. LDAP 过滤器示例

*作为管理员，您可以创建 **LDAP** 过滤器来限制特定用户对 **Satellite** 的访问。*

表 13.4. 允许特定用户登录的过滤器示例

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 目录结构

*示例中过滤器使用的 **LDAP** 目录结构：*

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

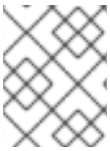
LDAP 组成员资格

示例中的过滤器使用的组成员资格：

组	成员
Group1	User1, User3
Group2	User2, User3

13.2. 使用 RED HAT IDENTITY MANAGEMENT

本节演示了如何将红帽卫星服务器与红帽身份管理服务器集成，以及如何启用基于主机的访问控制。



注意

您可以将红帽身份管理作为外部身份验证源附加，且无单点登录支持。更多信息请参阅第 13.1 节 “使用 LDAP”。

先决条件

- *Satellite 服务器必须在 Red Hat Enterprise Linux 7.1 或更高版本上运行。*
- *Satellite 服务器的基本操作系统必须注册到红帽身份管理域中。*

本章示例假设在 Red Hat Identity Management 和 Satellite 配置间分离。但是，如果您对两个服务器具有管理员特权，可以配置红帽身份管理，如 Red Hat Enterprise Linux 7 Linux 域身份、身份验证和策略指南 中所述。

13.2.1. 在卫星服务器上配置红帽身份管理身份验证

在卫星 CLI 中，首先在红帽身份管理服务器上创建主机条目来配置红帽身份管理身份验证。

流程

1. *在 Red Hat Identity Management 服务器中要进行身份验证，请输入以下命令并在提示时输入您的密码：*

```
# kinit admin
```

2. *要验证您是否已通过身份验证，请输入以下命令：*

```
# klist
```

3. *在 Red Hat Identity Management 服务器上，为 Satellite 服务器创建一个主机条目并生成一次性密码，例如：*

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

注意

必须在客户端中使用生成的一次性密码来完成 Red Hat Identity Management-enrollment。

有关主机配置属性的更多信息，请参阅 Red Hat Enterprise Linux 7 Linux 域身份、身份验证和策略指南中的关于 主机条目 配置属性。

4. *为 Satellite 服务器创建 HTTP 服务，例如：*

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

有关管理服务的更多信息，请参阅 Red Hat Enterprise Linux 7 Linux 域身份、身份验证和策略指南中的管理服务。https://access.redhat.com/documentation/zh-cn/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/s

5. *在 Satellite 服务器中安装 IPA 客户端：*

警告

此命令可能会在安装软件包的过程中重启 Satellite 服务。有关在 Satellite 中安装和更新软件包的详情，请参考 第 11.5 节 "在 Satellite 或 Capsule 的基本操作系统上管理软件包"。

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

6. *在卫星服务器上，以 root 用户身份输入以下命令来配置 Red Hat Identity Management-enrollment:*

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

使用 Red Hat Identity Management 管理员提供的一次性密码替换 OTP。

7. *如果 Satellite 服务器在 Red Hat Enterprise Linux 7 上运行，请执行以下命令：*

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

*安装程序依赖于 Red Hat Enterprise Linux 7 上的软件包，它们位于 **rhel-7-server-optional-rpms** 的可选存储库中。*

8. *使用以下命令将 **foreman-ipa-authentication** 设置为 true：*

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

9. *重启 **satellite-maintain** 服务：*

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

外部用户现在可以使用其红帽身份管理凭证登录 Satellite。现在，他们可以选择直接使用其用户名和密码直接登录卫星服务器，或者利用配置的 Kerberos 单点登录并在其客户端机器上获取一个 ticket，并自动登录。还支持使用一次性密码(2FA OTP)的双因素验证。如果为 2FA 配置了红帽身份管理中的用户，且卫星服务器在 Red Hat Enterprise Linux 7 上运行，此用户还可以使用 OTP 对 Satellite 进行身份验证。

13.2.2. 配置基于主机的验证控制

HBAC 规则定义允许 Red Hat Identity Management 用户访问哪些机器。您可以在红帽身份管理服务器上配置 HBAC，以防止选择的用户访问卫星服务器。通过这种方法，您可以防止 Satellite 为不允许登录的用户创建数据库条目。有关 HBAC 的更多信息，请参阅 Red Hat Enterprise Linux 7 Linux 域身份、身份验证和策略 指南中的配置基于主机的访问控制。

在红帽身份管理服务器上，配置基于主机的验证控制(HBAC)。

流程

1. 在 Red Hat Identity Management 服务器中要进行身份验证，请输入以下命令并在提示时输入您的密码：

```
# kinit admin
```

2. 要验证您是否已通过身份验证，请输入以下命令：

```
# klist
```

3. 在 Red Hat Identity Management 服务器上创建 HBAC 服务和规则，并将它们链接到一起。以下示例使用 PAM 服务名称 satellite-prod。在 Red Hat Identity Management 服务器中执行以下命令：

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

4. 添加要有权访问服务 satellite-prod 和 Satellite Server 主机名的用户：

```
# ipa hbacrule-add-user allow_satellite_prod --user=username
# ipa hbacrule-add-host allow_satellite_prod --hosts=satellite.example.com
```

或者，也可以将主机组和用户组添加到 allowsatellite_prod_ 规则。

5. 要检查规则的状态，请执行：

```
# ipa hbacrule-find satellite-prod
# ipa hbactest --user=username --host=satellite.example.com --service=satellite-prod
```

6. 确保 Red Hat Identity Management 服务器上禁用 allow_all 规则。有关如何在不中断其他服务的情况下进行此操作的步骤，请参阅红帽客户门户网站中的 IdM 中的如何配置 HBAC 规则。

7. 配置红帽身份管理与卫星服务器集成，如 第 13.2.1 节 “在卫星服务器上配置红帽身份管理身份验证” 所述。在卫星服务器上，以 root 用户身份定义 PAM 服务：

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

13.3. 使用 ACTIVE DIRECTORY

本节演示了如何使用直接 Active Directory(AD) 作为卫星服务器的外部身份验证源。

注意

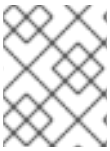
您可以将 Active Directory 附加为外部身份验证源，且无单点登录支持。更多信息请参阅 第 13.1 节 “使用 LDAP”。有关配置示例，请参阅 如何在 Satellite 6 上使用 TLS 配置 Active Directory 身份验证。

直接 AD 集成意味着卫星服务器直接加入到存储了身份的 AD 域。推荐的设置由两个步骤组成：

- 将卫星服务器注册到 Active Directory 服务器，如 第 13.3.2 节 “将 Satellite 服务器注册到 AD 服务器” 所述。
- 如 第 13.3.3 节 “使用 GSS-proxy 配置 Direct AD 集成”所述配置直接 Active Directory 与 GSS-proxy 集成。

13.3.1. GSS-Proxy

在 Apache 中，传统的 Kerberos 身份验证过程要求 Apache 进程具有 keytab 文件的读访问权限。GSS-Proxy 允许您通过删除 keytab 文件对 Apache 服务器进行更严格的权限分离，同时保留 Kerberos 身份验证功能。当使用 AD 作为 Satellite 的外部身份验证源时，建议实现 GSS-proxy，因为 keytab 文件中的密钥与主机密钥相同。



注意

AD 集成需要在 Red Hat Enterprise Linux 7.1 或更高版本上部署 Red Hat Satellite Server。

在作为卫星服务器的基础操作系统的红帽企业 Linux 上执行以下步骤。对于本节中的示例，EXAMPLE.ORG 是 AD 域的 Kerberos 域。完成操作后，属于 EXAMPLE.ORG 域的用户可以登录到卫星服务器。

13.3.2. 将 Satellite 服务器注册到 AD 服务器

在 Satellite CLI 中，将卫星服务器注册到 Active Directory 服务器。

先决条件

- 已安装 GSS-proxy 和 nfs-utils。
  安装 GSS-proxy 和 nfs-utils：

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

流程

1. 安装所需的软件包：

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

2. 将卫星服务器注册到 AD 服务器。您可能需要具有管理员权限才能执行以下操作：

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

13.3.3. 使用 GSS-proxy 配置 Direct AD 集成

在 Satellite CLI 中，配置直接 Active Directory 与 GSS-proxy 集成。

前提条件

- Satellite 与 Active Directory 服务器一起注册。
  更多信息请参阅 第 13.3.2 节 "将 Satellite 服务器注册到 AD 服务器"。

流程

1. 创建 **/etc/ipa/** 目录和 **default.conf** 文件：

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

2. 在 **default.conf** 文件中添加以下内容：

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

3. 使用以下内容创建 **/etc/net-keytab.conf** 文件：

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

4. 确定 Apache 用户的有效用户 ID：

```
# id apache
```

Apache 用户不能访问 keytab 文件。

5. 使用以下内容创建 **/etc/gssproxy/00-http.conf** 文件：

```
[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. 创建 keytab 条目：

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

```
# chmod 640 /etc/httpd/conf/http.keytab
```

7. 在 Satellite 中启用 IPA 验证：

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

8. 启动并启用 **gssproxy** 服务：

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

9. 将 Apache 服务器配置为使用 gssproxy 服务：

   a. 使用以下内容创建 **/etc/systemd/system/httpd.service** 文件：

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

   b. 对服务应用更改：

```
# systemctl daemon-reload
```

10. 启动并启用 **httpd** 服务：

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

11. 验证 SSO 是否按预期工作。
在运行 Apache 服务器时，如果客户端具有有效的 Kerberos 票据，则发出对服务器的 HTTP 请求的用户会被身份验证。

   a. 使用以下命令检索 LDAP 用户的 Kerberos ticket：

```
# kinit ldapuser
```

   b. 使用以下命令查看 Kerberos ticket：

```
# klist
```

   c. 使用以下命令，查看成功基于 SSO 的身份验证的输出：

```
# curl -k -u : --negotiate https://satellite.example.com/users/extlogin
```

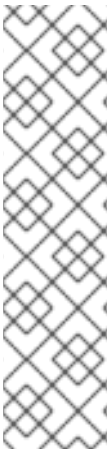
   这会返回以下响应：

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

13.3.4. Web 浏览器中的 Kerberos 配置

有关配置 Firefox 浏览器的详情，请参考 Red Hat Enterprise Linux System-Level 身份验证 指南中的将 Firefox 配置为使用 Kerberos 作为单点登录。

如果使用 Internet Explorer 浏览器，请将卫星服务器添加到 Local Intranet 或受信任的站点列表中，并打开" 启用集成 Windows 身份验证"设置。详情请查看 Internet Explorer 文档。



注意

对于直接 AD 集成，无法通过红帽身份管理提供 HBAC。作为替代方案，您可以使用组策略对象(GPO)，使管理员能够在 AD 环境中集中管理策略。要确保 GPO 服务映射正确，请使用以下 sssd 配置：

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

在这里，foreman 是 PAM 服务名称。有关 GPO 的更多信息，请参阅Red Hat Enterprise Linux Windows 集成指南。

13.3.5. 带有 Cross-Forest Trust 的 Active Directory

Kerberos 可以创建 跨林信任，定义两个其他两个不同域林之间的关系。域林是域层次结构，AD 和红帽身份管理都是一个林的。在 AD 和 Red Hat Identity Management 间启用了信任关系，AD 用户可以使用一组凭证访问 Linux 主机和服务。有关跨林信任的更多信息，请参阅 Red Hat Enterprise Linux Windows 集成 指南中的使用Active Directory 和 Identity Management 创建 Cross-forest Trusts。

从卫星的角度来看，配置过程与红帽身份管理服务器集成，无需配置跨林信任。Satellite Server 必须注册到 IPM 域并集成，如 第 13.2 节 “使用 Red Hat Identity Management”所述。

13.3.6. 将红帽身份管理服务器配置为使用 Cross-Forest Trust

在红帽身份管理服务器上，配置服务器以使用 跨林信任。

流程

1. 启用 HBAC：
   a. 创建一个外部组，并将 AD 组添加到其中。
   b. 将新的外部组添加到 POSIX 组。
   c. 在 HBAC 规则中使用 POSIX 组。
2. 配置 sssd 以传输 AD 用户的其他属性。
   - 将 AD 用户属性添加到 /etc/sssd/sssd.conf 中的nss 和domain 部分。
     例如：

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

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

13.4. 配置外部用户组

卫星不会自动将外部用户与其用户组相关联。您必须在 Satellite 上的外部源中创建名称与名称相同的用户组。然后，外部用户组的成员自动成为卫星用户组的成员并接收相关的权限。

外部用户组的配置取决于外部身份验证的类型。

要为外部用户分配附加权限，请将此用户添加到没有指定外部映射的内部用户组。然后，将所需的角色分配给此组。

先决条件

- 如果使用 LDAP 服务器，请将 Satellite 配置为使用 LDAP 身份验证。更多信息请参阅 第 13.1 节 "使用 LDAP"。
  使用 LDAP 源的外部用户组时，您不能使用 **$login** 变量作为帐户用户名的替换。您必须使用匿名或专用服务用户。
- 如果您使用 Red Hat Identity Management 或 AD 服务器，将 Satellite 配置为使用 Red Hat Identity Management 或 AD 身份验证。更多信息请参阅 第 13 章 配置外部身份验证。
- 首次确保至少有一个外部用户进行身份验证。
- 保留您要使用的外部组名称的副本。要查找外部用户的组成员资格，请输入以下命令：

```
# id username
```

配置外部用户组：

1. 在 Satellite Web UI 中，导航到 **Administer > User Groups**，然后单击 **Create User Group**。
2. 指定新用户组的名称。不要选择任何用户，以避免在刷新外部用户组时自动添加用户。
3. 单击 **Roles** 选项卡，再选择您要分配给该用户组的角色。或者，选择 **Administrator** 复选框来分配所有可用权限。
4. 单击 **External groups** 选项卡，然后单击 **Add external user group**，然后从 **Auth source** 下拉菜单中选择身份验证源。
   在 **Name** 字段中指定外部组的确切名称。
5. 点 **Submit**。

13.5. 为 LDAP 刷新外部用户组

要在 **Auth Source** 页面中将 LDAP 源设置为在用户登录时自动同步用户组成员资格，请选择 **Usergroup Sync** 选项。如果没有选择此选项，则默认情况下，LDAP 用户组会通过调度的 **cron** 作业自动刷新每 30 分钟同步 LDAP 身份验证源。

如果 LDAP 身份验证源中的用户组在调度的任务间发生了变化，用户可以将用户分配给不正确的外部用户组。当调度的任务运行时，它会被自动更正。

使用此流程手动刷新 LDAP 源。

流程

1. 导航到 **Administer > Usergroups** 并选择一个用户组。
2. 导航到 **External Groups** 选项卡，再单击 **Refresh to the required user group** 右侧的。

CLI 过程

- *输入以下命令：*

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

13.6. 为红帽身份管理或 AD 刷新外部用户组

仅在 Satellite 中的组成员登录时，基于 Red Hat Identity Management 或 AD 的外部用户组才会刷新。在卫星 Web UI 中无法更改外部用户组的用户成员资格，在下一次组刷新时可能会覆盖此类更改。

13.7. PROVISIONED 主机的外部身份验证

使用这个部分为红帽身份管理域支持配置卫星服务器或胶囊服务器，然后将主机添加到红帽身份管理域组中。

先决条件

您需要以下设置来为置备的主机配置外部身份验证：

- *注册到 Content Delivery Network 或注册到卫星服务器的外部胶囊服务器。*
- *已部署的域或域提供程序，如红帽身份管理。*

要在 Red Hat Satellite Server 或 Red Hat Satellite Capsule Server 上安装和配置红帽身份管理软件包：

要使用 Red Hat Identity Management 进行置备的主机，请完成以下步骤，在 Red Hat Satellite Server 或 Red Hat Satellite Capsule Server 上安装和配置 Red Hat Identity Management 软件包：

1. *在 Satellite 服务器或 Capsule Server 上安装 **ipa-client** 软件包：*

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

2. *将服务器配置为 Red Hat Identity Management 客户端：*

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

3. *在 Red Hat Identity Management 中创建 realm 代理用户、**realm-capsule** 以及相关的角色：*

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

   请注意返回和您的 Red Hat Identity Management 服务器配置详情的主体名称，因为您需要以下过程。

为红帽身份管理域配置 Satellite 服务器或胶囊服务器：

在 Satellite 上完成以下步骤以及您要使用的每个胶囊：

1. *将 **/root/freeipa.keytab** 文件复制到您要在同一主体和域中包含的任何胶囊服务器：*

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

2. 将 /root/freeipa.keytab 文件移到 /etc/foreman-proxy 目录，并将所有权设置设置为 foreman-proxy 用户：

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

3. 在域中包含的所有胶囊上输入以下命令。如果您在 Satellite 上使用集成胶囊，请在卫星服务器上输入以下命令：

```
# 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
```

   在首次配置红帽卫星服务器时，也可以使用这些选项。

4. 确保安装了 ca-certificates 软件包的最新版本，并信任 Red Hat Identity Management 证书颁发机构：

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

5. 可选：如果您在现有 Satellite 服务器或胶囊服务器上配置红帽身份管理，请完成以下步骤以确保配置更改生效：

   a. 重启 foreman-proxy 服务：

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

   b. 在 Satellite Web UI 中，导航到 Infrastructure > Capsules。

   c. 找到您为红帽身份管理配置的胶囊，并从 Actions 列中的列表中选择 Refresh。

要为启用了红帽身份管理胶囊创建域

在使用红帽身份管理配置集成或外部胶囊后，您必须创建一个域，并将红帽身份管理配置胶囊添加到域中。

要创建域，请完成以下步骤：

1. 在 Satellite Web UI 中，导航到 Infrastructure > Realms，再点击 Create Realm。
2. 在 Name 字段中输入域的名称。
3. 从 Realm Type 列表中，选择 realm 的类型。
4. 在 Realm Capsule 列表中，选择您配置 Red Hat Identity Management 的 Capsule Server。
5. 单击位置选项卡，从 位置 列表中选择要添加新域的位置。
6. 单击 Organizations 选项卡，再从 Organizations 列表中选择要添加新域的组织。
7. 点 Submit。

使用 Realm Information 更新主机组

您必须更新要与新域信息搭配使用的任何主机组。

1. 进入 **Configure >Host Groups**，选择您要更新的主机组，然后点击 **Network** 选项卡。
2. 在 **Realm** 列表中，选择您创建的域作为此流程的一部分，然后单击 **Submit**。

将主机添加到红帽身份管理主机组

Red Hat Identity Management 支持根据系统的属性设置自动成员资格规则。红帽卫星的域功能为管理员提供了将红帽卫星主机组映射到红帽身份管理参数 **用户类** 的功能，让管理员能够配置自动成员。

当使用嵌套式主机组时，它们将发送到红帽身份管理服务器，就像在 **Red Hat Satellite** 用户界面中显示一样。例如："Parent/Child/Child"。

卫星服务器或胶囊服务器会向红帽身份管理服务器发送更新，但自动成员规则仅在初始注册时应用。

要将主机添加到红帽身份管理主机组中：

1. 在 **Red Hat Identity Management** 服务器中创建一个主机组：

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

2. 创建 **自动成员** 规则：

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

   您可以使用以下选项：

   - ***automember-add*** 将组标记为 **automember** 组。
   - ***--type=hostgroup*** 确定目标组是主机组，而不是用户组。
   - ***automember_rule*** 会添加您要识别自动成员规则的名称。

3. 根据 ***userclass*** 属性定义自动成员条件：

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

   您可以使用以下选项：

   - ***automember-add-condition*** 添加正则表达式条件来识别组成员。
   - ***--key=userclass*** 将 **key** 属性指定为 ***userclass***。
   - ***--type=hostgroup*** 确定目标组是主机组，而不是用户组。
   - ***--inclusive-regex= ^webserver*** 使用正则表达式模式匹配值。

- hostgroup_name - 标识目标主机组的名称。

当系统添加到卫星服务器的hostgroup_name 主机组中时，它会自动添加到红帽身份管理服务器的 "hostgroup_name " 主机组中。Red Hat Identity Management 主机组允许基于主机的访问控制 (HBAC)、sudo 策略和其他红帽身份管理功能。

13.8. 使用 RED HAT SINGLE SIGN-ON 身份验证配置 SATELLITE

使用这个部分将卫星配置为使用红帽单点登录作为外部身份验证的 OpenID 提供程序。

13.8.1. 使用红帽单点登录身份验证配置 Satellite 的先决条件

在使用 Red Hat Single Sign-On 外部验证配置 Satellite 前，请确定您满足以下要求：

- 工作安装使用 HTTPS 而不是 HTTP 的 Red Hat Single Sign-On 服务器。
- 具有管理特权的 Red Hat Single Sign-On 帐户。
- 在红帽单点登录中创建的 Satellite 用户帐户的域。
- 如果证书或 CA 是自签名的，请确保将其添加到最终用户证书信任存储中。
- 导入或添加到红帽单点登录的用户。
  如果您配置了现有用户数据库，如 LDAP 或 Kerberos，您可以通过配置用户联合来导入用户。如需更多信息，请参阅 Red Hat Single Sign-On Server 管理指南 中的用户存储 创建器。

  如果您没有配置现有用户数据库，可以在 Red Hat Single Sign-On 中手动创建用户。如需更多信息，请参阅 Red Hat Single Sign-On Server 管理指南 中的创建新用户。https://access.redhat.com/documentation/zh-cn/red_hat_single_sign-on/7.4/html/server_administration_guide/user_management#create-new-user

13.8.2. 将 Satellite 注册为红帽单点登录客户端

使用这个步骤将 Satellite 注册到 Red Hat Single Sign-On 作为客户端，并将 Satellite 配置为使用 Red Hat Single Sign-On 作为身份验证源。

您可以使用两个不同的身份验证方法配置 Satellite 和 Red Hat Single Sign-On：

1. 用户使用卫星 Web UI 验证卫星。
2. 用户使用 Satellite CLI 对 Satellite 进行身份验证。

您必须决定用户提前验证，因为这两种方法都需要注册到 Red Hat Single Sign-On 并配置了不同的卫星客户端。在 Red Hat Single Sign-On 中注册和配置 Satellite 客户端的步骤可区分在过程中。

如果要使用身份验证方法并相应地配置这两个客户端，您也可以将两个不同的卫星客户端注册到 Red Hat Single Sign-On。

流程

1. 在 Satellite 服务器中安装以下软件包：

```
# satellite-maintain packages install mod_auth_openidc keycloak-httpd-client-install
```

2. 将 Satellite 注册到红帽单点登录作为客户端。请注意，您使用 Web UI 和 CLI 登录的注册过程有所不同。您可以将两个客户端注册到红帽单点登录，以便能够通过 Web UI 和 CLI 登录卫星。

   - 如果您希望用户使用 Web UI 验证 Satellite，请按如下所示创建客户端：

     ```
     # keycloak-httpd-client-install --app-name foreman-openidc \
     --keycloak-server-url "https://RHSSO.example.com" \
     --keycloak-admin-username "admin" \
     --keycloak-realm "Satellite_Realm" \
     --keycloak-admin-realm master \
     --keycloak-auth-role root-admin \
     -t openidc -l /users/extlogin --force
     ```

     在提示时输入 manage 帐户的密码。此命令会在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

     然后，将 Satellite 配置为使用 Red Hat Single Sign-On 作为身份验证源：

     ```
     # satellite-installer --foreman-keycloak true \
     --foreman-keycloak-app-name "foreman-openidc" \
     --foreman-keycloak-realm "Satellite_Realm"
     ```

   - 如果您希望用户通过 CLI 验证 Satellite，请按如下所示创建客户端：

     ```
     # keycloak-httpd-client-install --app-name hammer-openidc \
     --keycloak-server-url "https://RHSSO.example.com" \
     --keycloak-admin-username "admin" \
     --keycloak-realm "Satellite_Realm" \
     --keycloak-admin-realm master \
     --keycloak-auth-role root-admin \
     -t openidc -l /users/extlogin --force
     ```

     在提示时输入 manage 帐户的密码。此命令会在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

3. 重启 httpd 服务：

   ```
   # systemctl restart httpd
   ```

13.8.3. 在 Red Hat Single Sign-On 中配置 Satellite 客户端

使用这个步骤在 Red Hat Single Sign-On Web UI 中配置 Satellite 客户端，并为卫星客户端创建组和使用者映射程序。

流程

1. 在 Red Hat Single Sign-On Web UI 中，导航到 Clients 并单击 Satellite 客户端。

2. 配置访问类型：

   - 如果您希望用户使用 Web UI 向 Satellite 进行身份验证，从 Access Type 列表中选择 confidential。

   - 如果您希望用户使用 CLI 向 Satellite 进行身份验证，从 Access Type 列表中选择 public。

3. 在 Valid redirect URI 字段中，添加有效的重定向 URI。

   - 如果您希望用户使用 Web UI 验证 Satellite，在现有 URI 下的空白字段中，以 **https://satellite.example.com/users/extlogin** 格式输入 URI。请注意，您必须在 Satellite FQDN 之后添加字符串 **/users/extlogin**。
     完成此步骤后，使用 Web UI 登录的 Satellite 客户端必须具有以下 Valid Redirect URI ：

     ```
     https://satellite.example.com/users/extlogin/redirect_uri
     https://satellite.example.com/users/extlogin
     ```

   - 如果您希望用户使用 CLI 向 Satellite 进行身份验证，在现有 URI 下的空白字段中，输入 **urn:ietf:wg:oauth:2.0:oob**。
     完成此步骤后，使用 CLI 登录的 Satellite 客户端必须具有以下 Valid Redirect URI ：

     ```
     https://satellite.example.com/users/extlogin/redirect_uri
     urn:ietf:wg:oauth:2.0:oob
     ```

4. 点 Save。
5. 点 mappers 选项卡，然后点 Create 添加 audience mapper。
6. 在 Name 字段中输入 audience mapper 的名称。
7. 从 映射类型 列表中，选择 Audience。
8. 从 Included Client Audience 列表中，选择 Satellite 客户端。
9. 点 Save。
10. 点 Create 添加组映射程序，以便您可以根据组成员资格在 Satellite 中指定授权。
11. 在 Name 字段中输入组映射程序的名称。
12. 从 映射类型 列表中，选择 Group Membership。
13. 在 Token Claim Name 字段中输入组。
14. 将 Full group path 设置设为 OFF。
15. 点 Save。

13.8.4. 为红帽单点登录身份验证配置 Satellite 设置

使用这个部分，使用卫星 Web UI 或 CLI 为红帽单点登录身份验证配置 Satellite。

13.8.4.1. 使用 Web UI 为红帽单点登录身份验证配置 Satellite 设置

使用 Satellite Web UI 为红帽单点登录身份验证配置卫星设置。

请注意，您可以导航到域中的以下 URL，以获取配置 Satellite 设置的值：
https://RHSSO.example.com/auth/realms/Satellite_Realm/.well-known/openid-configuration

前提条件

- 确保 Red Hat Single Sign-On Web UI 中的 Satellite 客户端中的 Access Type 设置设为 机密

流程

1. 在 Satellite Web UI 中，导航到 Administer > Settings，然后点 Authentication 选项卡。
2. 找到 Authorize login delegation 行，然后在 Value 列中找到值设为 Yes。
3. 找到 Authorize login delegation auth source user autocreaterow，在 Value 列中，将值设为 External。
4. 找到 登录委托注销 URL 行，在 Value 列中，将值设为 https://satellite.example.com/users/extlogout。
5. 找到 OIDC Algorithm 行，在 Value 列中，将 Red Hat Single Sign-On 上的编码的算法设置为 RS256。
6. 找到 OIDC Audience 行，在 Value 列中，将值设置为 Red Hat Single Sign-On 的客户端 ID。
7. 找到 OIDC Issuer 行，在 Value 列中找到，将值设置为 https://RHSSO.example.com/auth/realms/Satellite_Realm。
8. 找到 OIDC JWKs URL 行，在 Value 列中，将值设置为 https://RHSSO.example.com/auth/realms/Satellite_Realm/protocol/openid-connect/certs。
9. 导航到 Administer > Authentication Sources，再点击 External。
10. 点击 Create LDAP Authentication Source 并选择 Red Hat Single Sign-On 服务器。
11. 单击位置选项卡，再添加可以使用红帽单点登录身份验证来源的位置。
12. 单击 Organizations 选项卡，再添加可以使用 Red Hat Single Sign-On 验证源的组织。
13. 点 Submit。

13.8.4.2. 使用 CLI 为红帽单点登录身份验证配置 Satellite 设置

使用此流程，通过 Satellite CLI 为红帽单点登录身份验证配置卫星设置。

请注意，您可以导航到域中的以下 URL，以获取配置 Satellite 设置的值：
https://RHSSO.example.com/auth/realms/Satellite_Realm/.well-known/openid-configuration

前提条件

- 确保 Red Hat Single Sign-On Web UI 中的 Satellite 客户端中的 Access Type 设置设为 public

流程

1. 在 Satellite 上，将登录委托设置为 **true**，以便用户可以使用 Open IDC 协议进行身份验证：

```
# hammer settings set --name authorize_login_delegation --value true
```

2. 设置登录委托注销 URL：

```
# hammer settings set --name login_delegation_logout_url \
--value https://satellite.example.com/users/extlogout
```

3. 在 Red Hat Single Sign-On 上设置编码的算法，如 **RS256** ：

```
# hammer settings set --name oidc_algorithm --value 'RS256'
```

4. 打开 **RHSSO.example.com/auth/realms/RHSSO_REALM/.well-known/openid-configuration URL**，并记录这些值以填充以下步骤中的选项。

5. 在 Open IDC 使用者中添加 Hammer 客户的值：

```
# hammer settings set --name oidc_audience \
--value "['satellite.example.com-hammer-openidc']"
```

注意

如果您将多个 Red Hat Single Sign-On 客户端注册到 Satellite，请确保在阵列中附加所有受众。例如：

```
# hammer settings set --name oidc_audience \
--value "['satellite.example.com-foreman-openidc', 'satellite.example.com-hammer-openidc']"
```

6. 设置 Open IDC 签发者的值：

```
# hammer settings set --name oidc_issuer \
--value "RHSSO.example.com/auth/realms/RHSSO_Realm"
```

7. 设置 Open IDC Java Web 令牌(JWT)的值：

```
# hammer settings set --name oidc_jwks_url \
--value "RHSSO.example.com/auth/realms/RHSSO_Realm/protocol/openid-connect/certs"
```

8. 检索 Red Hat Single Sign-On 验证源的 ID ：

```
# hammer auth-source external list
```

9. 设置位置和机构：

```
# hammer auth-source external update --id Authentication Source ID \
--location-ids Location ID --organization-ids Organization ID
```

13.8.5. 使用 Red Hat Single Sign-On 登录 Satellite Web UI

使用此流程，使用红帽单点登录登录卫星 Web UI。

流程

- 在您的浏览器中，登录 Satellite 并输入您的凭证。

13.8.6. 使用 Red Hat Single Sign-On 登录 Satellite CLI

使用此流程，通过代码授权类型对 Satellite CLI 进行身份验证。

流程

1. 要使用代码授权类型验证 Satellite CLI，请输入以下命令：

```
# hammer auth login oauth \
--two-factor \
--oidc-token-endpoint 'https://RHSSO.example.com/auth/realms/ssl-realm/protocol/openid-connect/token' \
--oidc-authorization-endpoint 'https://RHSSO.example.com/auth' \
--oidc-client-id 'satellite.example.com-foreman-openidc' \
--oidc-redirect-uri urn:ietf:wg:oauth:2.0:oob
```

   该命令提示您输入成功代码。

2. 要检索成功代码，请导航到命令返回并提供所需信息的 URL。
3. 复制 Web UI 返回的成功代码。
4. 在 **hammer auth login oauth** 命令提示符下，输入成功代码以向 Satellite CLI 进行身份验证。

13.8.7. 为红帽单点登录身份验证配置组映射

另外，要实施基于角色的访问控制(RBAC)，在 Satellite 中创建组，将角色分配给此组，然后将 Active Directory 组映射到 Satellite 组。因此，Red Hat Single Sign-On 中给定组中的任何人都登录在对应的 Satellite 组下。本例在 Active Directory 中配置 Satellite-admin 用户组的用户，以以具有卫星上具有管理员特权的用户进行身份验证。

流程

1. 在 Satellite Web UI 中，导航到 Administer > User Groups，然后单击 Create User Group 按钮。
2. 在 Name 字段中输入用户组群的名称。名称不应与 Active Directory 中的相同。
3. 不要在右列中添加用户和用户组。点 Roles 选项卡。
4. 选中 Administer 复选框。
5. 点 External Groups 选项卡。
6. 点 Add external user group。
7. 在 Name 字段中输入 Active Directory 组的名称。
8. 从列表中，选择 EXTERNAL。

13.9. 使用 TOTP 配置红帽单点登录身份验证

使用这个部分将 Satellite 配置为使用 Red Hat Single Sign-On 作为 OpenID 供应商，使用 TOTP 卡进行外部身份验证。

13.9.1. 使用红帽单点登录身份验证配置 Satellite 的先决条件

在使用 Red Hat Single Sign-On 外部验证配置 Satellite 前，请确定您满足以下要求：

- 工作安装使用 HTTPS 而不是 HTTP 的 Red Hat Single Sign-On 服务器。

- 具有管理特权的 Red Hat Single Sign-On 帐户。
- 在红帽单点登录中创建的 Satellite 用户帐户的域。
- 如果证书或 CA 是自签名的，请确保将其添加到最终用户证书信任存储中。
- 导入或添加到红帽单点登录的用户。
  如果您配置了现有用户数据库，如 LDAP 或 Kerberos，您可以通过配置用户联合来导入用户。如需更多信息，请参阅 Red Hat Single Sign-On Server 管理指南 中的用户存储 创建器。

  如果您没有配置现有用户数据库，可以在 Red Hat Single Sign-On 中手动创建用户。如需更多信息，请参阅 Red Hat Single Sign-On Server 管理指南 中的创建新用户。https://access.redhat.com/documentation/zh-cn/red_hat_single_sign-on/7.4/html/server_administration_guide/user_management#create-new-user

13.9.2. 将 Satellite 注册为红帽单点登录客户端

使用这个步骤将 Satellite 注册到 Red Hat Single Sign-On 作为客户端，并将 Satellite 配置为使用 Red Hat Single Sign-On 作为身份验证源。

您可以使用两个不同的身份验证方法配置 Satellite 和 Red Hat Single Sign-On：

1. 用户使用卫星 Web UI 验证卫星。
2. 用户使用 Satellite CLI 对 Satellite 进行身份验证。

您必须决定用户提前验证，因为这两种方法都需要注册到 Red Hat Single Sign-On 并配置了不同的卫星客户端。在 Red Hat Single Sign-On 中注册和配置 Satellite 客户端的步骤可区分在过程中。

如果要使用身份验证方法并相应地配置这两个客户端，您也可以将两个不同的卫星客户端注册到 Red Hat Single Sign-On。

流程

1. 在 Satellite 服务器中安装以下软件包：

```
# satellite-maintain packages install mod_auth_openidc keycloak-httpd-client-install
```

2. 将 Satellite 注册到红帽单点登录作为客户端。请注意，您使用 Web UI 和 CLI 登录的注册过程有所不同。您可以将两个客户端注册到红帽单点登录，以便能够通过 Web UI 和 CLI 登录卫星。

   - 如果您希望用户使用 Web UI 验证 Satellite，请按如下所示创建客户端：

```
# keycloak-httpd-client-install --app-name foreman-openidc \
--keycloak-server-url "https://RHSSO.example.com" \
--keycloak-admin-username "admin" \
--keycloak-realm "Satellite_Realm" \
--keycloak-admin-realm master \
--keycloak-auth-role root-admin \
-t openidc -l /users/extlogin --force
```

   在提示时输入 manage 帐户的密码。此命令会在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

   然后，将 Satellite 配置为使用 Red Hat Single Sign-On 作为身份验证源：

```
# satellite-installer --foreman-keycloak true \
--foreman-keycloak-app-name "foreman-openidc" \
--foreman-keycloak-realm "Satellite_Realm"
```

- 如果您希望用户通过 CLI 验证 Satellite，请按如下所示创建客户端：

```
# keycloak-httpd-client-install --app-name hammer-openidc \
--keycloak-server-url "https://RHSSO.example.com" \
--keycloak-admin-username "admin" \
--keycloak-realm "Satellite_Realm" \
--keycloak-admin-realm master \
--keycloak-auth-role root-admin \
-t openidc -l /users/extlogin --force
```

在提示时输入 manage 帐户的密码。此命令会在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

3. 重启 **httpd** 服务：

```
# systemctl restart httpd
```

13.9.3. 在 Red Hat Single Sign-On 中配置 Satellite 客户端

使用这个步骤在 Red Hat Single Sign-On Web UI 中配置 Satellite 客户端，并为卫星客户端创建组和使用者映射程序。

流程

1. 在 Red Hat Single Sign-On Web UI 中，导航到 Clients 并单击 Satellite 客户端。
2. 配置访问类型：
   - 如果您希望用户使用 Web UI 向 Satellite 进行身份验证，从 Access Type 列表中选择 **confidential**。
   - 如果您希望用户使用 CLI 向 Satellite 进行身份验证，从 Access Type 列表中选择 **public**。
3. 在 Valid redirect URI 字段中，添加有效的重定向 URI。
   - 如果您希望用户使用 Web UI 验证 Satellite，在现有 URI 下的空白字段中，以 **https://satellite.example.com/users/extlogin** 格式输入 URI。请注意，您必须在 Satellite FQDN 之后添加字符串 **/users/extlogin**。
     完成此步骤后，使用 Web UI 登录的 Satellite 客户端必须具有以下 Valid Redirect URI ：

     ```
     https://satellite.example.com/users/extlogin/redirect_uri
     https://satellite.example.com/users/extlogin
     ```

   - 如果您希望用户使用 CLI 向 Satellite 进行身份验证，在现有 URI 下的空白字段中，输入 **urn:ietf:wg:oauth:2.0:oob**。
     完成此步骤后，使用 CLI 登录的 Satellite 客户端必须具有以下 Valid Redirect URI ：

     ```
     https://satellite.example.com/users/extlogin/redirect_uri
     urn:ietf:wg:oauth:2.0:oob
     ```

4. 点 Save。
5. 点 mappers 选项卡，然后点 Create 添加 audience mapper。
6. 在 Name 字段中输入 audience mapper 的名称。
7. 从 映射类型 列表中，选择 Audience。
8. 从 Included Client Audience 列表中，选择 Satellite 客户端。
9. 点 Save。
10. 点 Create 添加组映射程序，以便您可以根据组成员资格在 Satellite 中指定授权。
11. 在 Name 字段中输入组映射程序的名称。
12. 从 映射类型 列表中，选择 Group Membership。
13. 在 Token Claim Name 字段中输入组。
14. 将 Full group path 设置设为 OFF。
15. 点 Save。

13.9.4. 为红帽单点登录身份验证配置 Satellite 设置

使用这个部分，使用卫星 Web UI 或 CLI 为红帽单点登录身份验证配置 Satellite。

13.9.4.1. 使用 Web UI 为红帽单点登录身份验证配置 Satellite 设置

使用 Satellite Web UI 为红帽单点登录身份验证配置卫星设置。

请注意，您可以导航到域中的以下 URL，以获取配置 Satellite 设置的值：
https://RHSSO.example.com/auth/realms/Satellite_Realm/.well-known/openid-configuration

前提条件

- 确保 Red Hat Single Sign-On Web UI 中的 Satellite 客户端中的 Access Type 设置设为 机密

流程

1. 在 Satellite Web UI 中，导航到 Administer > Settings，然后点 Authentication 选项卡。
2. 找到 Authorize login delegation 行，然后在 Value 列中找到值设为 Yes。
3. 找到 Authorize login delegation auth source user autocreaterow，在 Value 列中，将值设为 External。
4. 找到 登录委托注销 URL 行，在 Value 列中，将值设为 https://satellite.example.com/users/extlogout。
5. 找到 OIDC Algorithm 行，在 Value 列中，将 Red Hat Single Sign-On 上的编码的算法设置为 RS256。
6. 找到 OIDC Audience 行，在 Value 列中，将值设置为 Red Hat Single Sign-On 的客户端 ID。

7. 找到 OIDC Issuer 行，在 Value 列中找到，将值设置为 https://RHSSO.example.com/auth/realms/Satellite_Realm。
8. 找到 OIDC JWKs URL 行，在 Value 列中，将值设置为 https://RHSSO.example.com/auth/realms/Satellite_Realm/protocol/openid-connect/certs。
9. 导航到 Administer >Authentication Sources，再点击 External。
10. 点击 Create LDAP Authentication Source 并选择 Red Hat Single Sign-On 服务器。
11. 单击位置选项卡，再添加可以使用红帽单点登录身份验证来源的位置。
12. 单击 Organizations 选项卡，再添加可以使用 Red Hat Single Sign-On 验证源的组织。
13. 点 Submit。

13.9.4.2. 使用 CLI 为红帽单点登录身份验证配置 Satellite 设置

使用此流程，通过 Satellite CLI 为红帽单点登录身份验证配置卫星设置。

请注意，您可以导航到域中的以下 URL，以获取配置 Satellite 设置的值：
https://RHSSO.example.com/auth/realms/Satellite_Realm/.well-known/openid-configuration

前提条件

- 确保 Red Hat Single Sign-On Web UI 中的 Satellite 客户端中的 Access Type 设置设为 public

流程

1. 在 Satellite 上，将登录委托设置为 **true**，以便用户可以使用 Open IDC 协议进行身份验证：

```
# hammer settings set --name authorize_login_delegation --value true
```

2. 设置登录委托注销 URL：

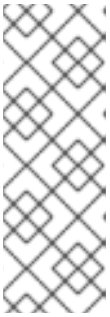
```
# hammer settings set --name login_delegation_logout_url \
--value https://satellite.example.com/users/extlogout
```

3. 在 Red Hat Single Sign-On 上设置编码的算法，如 **RS256**：

```
# hammer settings set --name oidc_algorithm --value 'RS256'
```

4. 打开 **RHSSO.example.com/auth/realms/RHSSO_REALM/.well-known/openid-configuration** URL，并记录这些值以填充以下步骤中的选项。
5. 在 Open IDC 使用者中添加 Hammer 客户的值：

```
# hammer settings set --name oidc_audience \
--value "['satellite.example.com-hammer-openidc']"
```



注意

如果您将多个 Red Hat Single Sign-On 客户端注册到 Satellite，请确保在阵列中附加所有受众。例如：

```
# hammer settings set --name oidc_audience \
--value "['satellite.example.com-foreman-openidc', 'satellite.example.com-hammer-openidc']"
```

6. *设置 Open IDC 签发者的值：*

```
# hammer settings set --name oidc_issuer \
--value "RHSSO.example.com/auth/realms/RHSSO_Realm"
```

7. *设置 Open IDC Java Web 令牌(JWT)的值：*

```
# hammer settings set --name oidc_jwks_url \
--value "RHSSO.example.com/auth/realms/RHSSO_Realm/protocol/openid-connect/certs"
```

8. *检索 Red Hat Single Sign-On 验证源的 ID：*

```
# hammer auth-source external list
```

9. *设置位置和机构：*

```
# hammer auth-source external update --id Authentication Source ID \
--location-ids Location ID --organization-ids Organization ID
```

13.9.5. 为 TOTP 身份验证配置 Red Hat Single Sign-On

使用这个流程将 Satellite 配置为使用 Red Hat Single Sign-On 作为 OpenID 供应商，使用基于时间的一次性密码(TOTP)进行外部身份验证。

流程

1. *在 Red Hat Single Sign-On Web UI 中，导航到 Satellite 域。*
2. *导航到 Authentication，点 OTP Policy 选项卡。*
3. *确保 支持的 Applications 字段包含 FreeOTP 或 Google Authenticator。*
4. *配置 OTP 设置以符合您的要求。*
5. *可选：如果要将 TOTP 身份验证用作所有用户的默认验证方法，点 Flows 选项卡，然后选择 OTP Form 设置的权利，请选择 REQUIRED。*
6. *点 所需的 Actions 选项卡。*
7. *在 Configure OTP 行的右侧，选择 Default Action 复选框。*

13.9.6. 使用 Red Hat Single Sign-On TOTP 身份验证登录到 Satellite Web UI

使用 Red Hat Single Sign-On TOTP 身份验证登录到 Satellite Web UI。

流程

1. 登录卫星，Satellite 重定向到红帽单点登录登录屏幕。
2. 输入您的用户名和密码，然后点击 Log In。
3. 首先尝试登录，通过扫描 barcode 并输入显示 pin，来配置您的客户端的红帽单点登录请求。
4. 在配置客户端并输入有效的 PIN 后，Red Hat Single Sign-On 会将您重定向到 Satellite 并登录。

13.9.7. 使用 Red Hat Single Sign-On 登录 Satellite CLI

使用此流程，通过代码授权类型对 Satellite CLI 进行身份验证。

流程

1. 要使用代码授权类型验证 Satellite CLI，请输入以下命令：

```
# hammer auth login oauth \
--two-factor \
--oidc-token-endpoint 'https://RHSSO.example.com/auth/realms/ssl-realm/protocol/openid-connect/token' \
--oidc-authorization-endpoint 'https://RHSSO.example.com/auth' \
--oidc-client-id 'satellite.example.com-foreman-openidc' \
--oidc-redirect-uri urn:ietf:wg:oauth:2.0:oob
```

   该命令提示您输入成功代码。

2. 要检索成功代码，请导航到命令返回并提供所需信息的 URL。
3. 复制 Web UI 返回的成功代码。
4. 在 **hammer auth login oauth** 命令提示符下，输入成功代码以向 Satellite CLI 进行身份验证。

13.9.8. 为红帽单点登录身份验证配置组映射

另外，要实施基于角色的访问控制(RBAC)，在 Satellite 中创建组，将角色分配给此组，然后将 Active Directory 组映射到 Satellite 组。因此，Red Hat Single Sign-On 中给定组中的任何人都登录在对应的 Satellite 组下。本例在 Active Directory 中配置 Satellite-admin 用户组的用户，以以具有卫星上具有管理员特权的用户进行身份验证。

流程

1. 在 Satellite Web UI 中，导航到 Administer > User Groups，然后单击 Create User Group 按钮。
2. 在 Name 字段中输入用户组群的名称。名称不应与 Active Directory 中的相同。
3. 不要在右列中添加用户和用户组。点 Roles 选项卡。
4. 选中 Administer 复选框。
5. 点 External Groups 选项卡。
6. 点 Add external user group。
7. 在 Name 字段中输入 Active Directory 组的名称。

8. 从列表中，选择 **EXTERNAL**。

13.10. 禁用 RED HAT SINGLE SIGN-ON 身份验证

如果要在 Satellite 中禁用 Red Hat Single Sign-On 身份验证，请完成此步骤。

流程

- 输入以下命令禁用 Red Hat Single Sign-On 身份验证：

```
# satellite-installer --reset-foreman-keycloak
```

第 14 章 监控资源

以下章节详细介绍了如何为受管系统配置监控和报告。这包括主机配置、内容视图、合规性、订阅、注册的主机、升级和同步。

14.1. 使用 RED HAT SATELLITE CONTENT DASHBOARD

Red Hat Satellite 内容仪表板包含各种小部件，它们提供了主机配置、内容视图、合规性报告、订阅和主机目前注册、升级和同步以及最新通知列表的概述。

导航到 **Monitor > Dashboard** 以访问内容仪表板。可以通过单击小部件并将它拖到不同的位置来重新排列仪表板。可用的小部件如下：

主机配置状态

配置状态概述以及最后一次报告间隔期间与之关联的主机数量。下表显示了可能的配置状态的描述。

表 14.1. 主机配置状态

图标	状态	描述
	执行修改的主机没有错误	在最后报告间隔期间成功执行了修改的主机。
	处于错误状态的主机	在最后报告间隔内检测到错误的主机。
	在过去的 35 分钟内报告良好主机	在最后 35 分钟内没有执行任何修改的主机。
	待处理的更改的主机	应用某些资源的主机，但 Puppet 已配置为在 **noop** 模式下运行。
	没有同步主机	未同步的主机并在最后报告间隔内收到报告。
	没有报告的主机	在最后报告间隔内未收集任何报告的主机。
	禁用警报的主机	未被监控的主机。

单击特定的配置状态，以查看与之关联的主机。

主机配置图

饼图显示配置状态的比例以及与其关联的所有主机的比例。

最新事件

主机生成的消息列表，包括管理信息、产品和订阅更改以及任何错误。
监控此部分，了解发送到所有用户的全局通知，并检测任何不常见的活动或错误。

运行发布（最后 30 分钟）

图显示最近 Puppet 间隔期间正在运行的 Puppet 代理的分布，默认为 30 分钟。在这种情况下，每个列都是在 3 分钟期间从客户端接收的大量报告。

新主机

最近创建的主机的列表。单击主机以获取更多详细信息。

任务状态

所有当前任务的摘要，按其状态和结果分组。点数字查看对应任务的列表。

最新警告/错误任务

因警告或错误而停止的最新任务列表。点一个任务来查看更多详情。

发现的主机

Discovery 插件在 provisioning 网络中检测到的所有裸机主机的列表。

最新勘误

注册到卫星中的主机所有可用勘误表的列表。

内容视图

卫星中的所有内容视图及其发布状态的列表。

同步概述

卫星中启用的所有产品或存储库及其同步状态的概述。队列中的所有产品都未同步，或者之前已同步过，本节将列出。

主机订阅状态

注册到 Satellite 的主机当前使用的订阅概述。订阅是一个购买的证书，可解锁主机对软件、升级和安全修复的访问。下表显示了订阅可能的状态。

表 14.2. 主机订阅状态

图标	状态	描述
	无效	主机已安装产品，但没有正确订阅产品。这些主机需要立即关注。
	部分	具有订阅和有效权利的主机，但没有使用其完整的权利。应监控这些主机以确保它们按预期配置。
	有效	具有有效权利且使用其完整权利的主机。

点订阅类型查看与所选类型订阅关联的主机。

订阅状态

显示当前订阅总数的概览，显示有效订阅的数量、下一个 120 天内过期的订阅数量，以及最近过期的订阅数量。

主机集合

Satellite 中的所有主机集合及其状态的列表，包括每个主机集合中的内容数量。

virt-who Configuration Status

*从环境中运行的 **virt-who** 守护进程中收到的报告状态概述。下表显示了可能的状态。*

表 14.3. virt-who Configuration States

状态	描述
没有报告	未收到报告，因为在 virt-who 配置部署期间发生错误，或者配置尚未部署，或者 virt-who 在计划的时间间隔期间无法连接到 Satellite。
没有更改	未收到报告，因为虚拟机监控程序没有检测到虚拟机的任何更改，或者 virt-who 在计划的时间间隔内无法上传报告。如果您添加了虚拟机，但配置处于 **No Change** 状态，请检查 virt-who。
确定	在调度的间隔内收到报告且无错误。
配置总数	virt-who 配置总数。

点配置状态查看这个状态的所有配置。

*小部件还在"不更改配置"下列出 **No Change state** 下的三个最新配置。*

最新合规性报告

最新合规性报告列表。每个合规性报告显示通过多个规则(P)、Failed(F)或其它ed(O)的规则。点主机获取详细的合规性报告。点击策略以了解更多详细信息。

合规性报告明细

饼图显示合规报告的分布根据其状态。

Red Hat Insights Actions

Red Hat Insights 是一个嵌入在 Satellite 中的工具，可检查环境并推荐您可以执行的操作。这个操作分为 4 个类别：可用性、稳定性、性能和安全性。

Red Hat Insights Risk Summary

表显示了根据风险级别的分发操作。风险级别代表了操作的关键程度以及造成实际问题的可能性。可能的风险等级为：Low、Medium、High 和 Critical。

注意

无法更改卫星 Web UI 中显示的日期格式。

14.1.1. 管理任务

*红帽卫星保留了所有计划或执行任务的完整日志，如已发布的存储库同步、应用勘误表和内容视图等。要查看日志，请导航到 **Monitor > Tasks**。*

在任务窗口中，您可以搜索特定的任务，查看其状态、详细信息以及自启动起所经过的时间。您还可以取消和恢复一个或多个任务。

这些任务使用 Dynflow 引擎进行管理。远程任务具有超时，可根据需要进行调整。

调整超时设置：

1. 进入 Administer > Settings。
2. 在搜索框中输入 %_timeout 并点 Search。搜索应该返回四个设置，包括描述。
3. 在 Value 列中，单击数字旁边的图标进行编辑。
4. 输入所需值（以秒为单位），然后单击 Save。

注意

在出现低带宽时，调整 %_finish_timeout 值可能会有所帮助。在出现高延迟时，调整 %_accept_timeout 值可能会有所帮助。

初始化任务后，将检查任务中使用的任何后端服务，如 Candlepin 或 Pulp，以便检查正确运行。如果检查失败，您将收到类似如下的错误：

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

如果后端服务检查功能造成任何问题，可以禁用它，如下所示。

禁用服务的检查：

1. 进入 Administer > Settings。
2. 在搜索框中输入 check_services_before_actions，然后点击 Search。
3. 在 Value 列中，单击图标以编辑该值。
4. 从下拉菜单中选择 false。
5. 点 Save。

14.2. 配置 RSS 通知

要查看 Satellite 事件通知警报，请单击屏幕右上角的 Notifications 图标。

默认情况下，Notifications 区域会显示 Red Hat Satellite Blog 中发布的 RSS 源事件。

反馈将每 12 小时刷新一次，每当新事件可用时，通知区域都会更新。

您可以通过更改 URL 源来配置 RSS 源通知。支持的源格式为 RSS 2.0 和 Atom。有关 RSS 2.0 源结构的示例，请参阅 Red Hat Satellite Blog feed。有关 Atom 源结构的示例，请参阅 Foreman 博客源。

要配置 RSS Feed 通知：

1. 导航到 Administer > Settings 并选择 Notifications 选项卡。
2. 在 RSS URL 行中，单击 Value 列中的编辑图标，然后键入所需的 URL。

3. 在 RSS enable 行中，单击 Value 列中的编辑图标，以启用或禁用此功能。

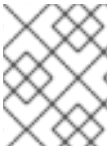
14.3. 监控 SATELLITE 服务器

在 Satellite Server Web UI 中的 About 页面中，您可以找到以下概述：

- 系统状态，包括胶囊、可用提供程序、计算资源和插件
- 支持信息
- 系统信息
- 后端系统状态
- 安装的软件包

进入 About 页面：

- 在 Satellite Server Web UI 的右上角，点 Administer > About。



注意

在 Pulp 失败后，因为同步延迟，Pulp 的状态可能会显示 OK，而不是 Error for up 10 分钟。

14.4. 监控胶囊服务器

下面的部分演示了如何使用卫星 Web UI 查找对维护和故障排除有价值的胶囊信息。

14.4.1. 查看常规胶囊信息

导航到 Infrastructure > Capsules，以查看注册到卫星服务器的胶囊服务器表。表中包含的信息回答了以下问题：

胶囊服务器是否在运行？

这通过 Status 列中的一个绿色图标表示。一个红色图标表示一个不活跃的胶囊，在 Capsule Server 上使用 服务 **foreman-proxy restart** 命令来激活它。

胶囊服务器上启用了哪些服务？

在 Features 列中，您可以验证 等胶囊是否提供 DHCP 服务或充当 Pulp 镜像。也可以在安装过程中启用或配置胶囊功能。如需更多信息，请参阅安装胶囊服务器。

胶囊式服务器分配到什么组织和位置？

胶囊服务器可以分配到多个组织和位置，但仅显示属于当前选定组织的胶囊。若要列出所有胶囊，请从左上角的上下文菜单中选择 Any Organization。
在更改胶囊配置后，从 Actions 列中的下拉菜单中选择 Refresh，以确保 Capsule 表 up to date。

单击 Capsule name 以查看其他详细信息。在 Overview 选项卡中，您可以在 Capsule 表中找到与 相同的信息。另外，您可以回答以下问题：

哪些主机由胶囊服务器管理？

Hosts managed 标签旁边显示关联的主机数量。单击该数字，以查看关联主机的详细信息。

胶囊服务器上有多少存储空间？

此时会显示由 /var/lib/pulp 中的 Pulp 内容所占用的存储空间量。另外，胶囊上的其余可用空间也可以被确定。

14.4.2. 监控服务

导航到 Infrastructure > Capsules，再单击所选 Capsule 的名称。在 Services 选项卡中，您可以查找胶囊服务（如 DNS 域列表或 Pulp worker 的列表）的基本信息。页面的外观取决于在胶囊服务器上启用了哪些服务。提供更详细的状态信息的服务可以在 Capsule 页面中具有专用标签页（请参阅 第 14.4.3 节 "监控 Puppet"）。

14.4.3. 监控 Puppet

导航到 Infrastructure > Capsules，再单击所选 Capsule 的名称。在 Puppet 标签页上，您可以找到以下内容：

- Puppet 事件摘要、最新 Puppet 运行概述以及 常规 子选项卡相关主机的同步状态。
- 环境子选项卡中的 Puppet 环境 列表。

在 Puppet CA 选项卡中，您可以找到以下内容：

- 证书状态概述以及 常规 子选项卡上的自动签名条目数。
- 与在证书子选项卡中的胶囊关联的 CA 证书 表。在这里，您可以检查证书到期数据，或者点击 Revoke 来取消证书。
- Autosign 条目子选项卡上的自动签名条目列表。在这里，您可以通过单击 New 或删除条目，只需单击 Delete 即可。

第 15 章 使用 WEBHOOK

Webhook 是网页或 Web 应用程序以实时为其他应用程序提供信息的方法。Webhook 仅在事件发生后触发。请求通常包含事件的详细信息。事件触发回调，如发送电子邮件确认主机已置备。Webhook 允许您使用 fire-and-forget 消息交换模式，基于卫星内部事件定义对外部 API 的调用。发送请求的应用程序不会等待响应，或忽略它。

Webhook 模板的有效负载是从 Webhook 模板创建的。Webhook 模板使用与 Provisioning 模板相同的 ERB 语法。可用变量：

- **@event_name**: 事件的名称。
- **@webhook_id**: unique event ID。
- **@payload**: Payload 数据，每种事件类型的不同。要访问个别字段，请使用 **@payload[:key_name]** Ruby hash 语法。
- **@payload[:object]**: Database 对象用于数据库操作触发的事件（create、update、delete）。不适用于自定义事件。
- **@payload[:context]**：其他信息作为散列，如请求和会话 UUID、远程 IP 地址、用户、机构和位置。

由于 Webhook 使用 HTTP，因此不需要向现有 Web 服务添加新基础架构。

Satellite 中 Webhook 的典型用例是在创建或删除主机时调用监控系统。

Webhook 可用于外部系统中要执行的操作，可以通过其 API 来完成。如果需要运行其他命令或编辑文件，则可使用 Capsules 的 shellhooks 插件。shellhooks 插件允许您在胶囊上定义可通过 API 执行的 shell 脚本。

您可以在不安装 shellhooks 插件的情况下成功使用 Webhook。

有关可用事件的列表，请参阅 可用的 Webhook 事件。

15.1. 迁移到 WEBHOOK

传统的 **foreman_hooks** 插件提供了对 webhook 插件不有意提供的模型对象的完整访问权限。

可用的范围受安全模式和所有对象及宏的限制，它们都受到 API 稳定性承诺的约束，并且已完全记录。

Webhook 触发的事件数量显著低于 **foreman_hooks**。

Webhook 异步处理，因此对系统的内部修改风险最少。无法从 **foreman_hooks** 迁移，而不会为每个单独 webhook 脚本创建有效负载。但是，webhook 插件带有几个示例有效负载模板。您还可以将示例有效负载与 shellhook 一起使用来简化迁移。

必须自定义脚本和有效负载模板才能实现类似结果。

15.2. 安装 WEBHOOK

使用以下步骤安装 Webhook。安装 Webhook 后，您可以将 Satellite 服务器配置为发送 Webhook 请求。

流程

- 使用以下命令安装 Webhook：

```
# satellite-installer --enable-foreman-plugin-webhooks
```

- 另外，您可以使用以下命令安装 CLI 插件：

```
# yum install tfm-rubygem-hammer_cli_foreman_webhooks
```

15.3. 创建 WEBHOOK 模板

使用以下步骤在卫星 Web UI 中创建 Webhook 模板。

流程

1. 在 Satellite Web UI 中，导航到 Administer > Webhooks Templates。
2. 点 Clone an existing template 或 Create Template。
3. 输入模板的名称。
4. 使用编辑器对模板有效负载进行更改。
   Webhook HTTP 有效负载必须使用 Satellite 模板语法创建。Webhook 模板可以使用一个名为 **@object** 的特殊变量，它可以代表事件的主对象。

   如需更多信息，请参阅 管理 主机和可用模板宏和方法中的模板编写参考，请参阅卫星服务器上的 **/templates_doc**。
5. 可选：输入描述和审核注释。
6. 分配组织和位置。
7. 点 Submit。

15.4. 创建 WEBHOOK

您可以通过 Satellite Web UI 自定义事件、有效负载、HTTP 身份验证、内容类型和标头。

使用以下步骤在卫星 Web UI 中创建 Webhook。

流程

1. 在 Satellite Web UI 中，点 Administer > Webhooks。
2. 点 Create Webhook。
3. 点击 Subscribe 选择事件。
4. 输入名称。
5. 输入目标 URL。Webhook 发出 HTTP 请求来预先配置的 URL。目标 URL 可以是动态 URL。使用 shellhooks 插件时，URL 应采用 **https://capsule.example.com:9090/shellhook/my_script** 格式。
6. 单击 Template 以选择模板。

7. 输入 HTTP 方法。
8. 如果要创建活跃的 Webhook，请检查 Enabled 标记。
9. 点 Credentials 选项卡。
10. 可选：如果需要使用 HTTP 验证，请输入用户名和密码。
11. 如果应针对系统证书存储或 Satellite CA 验证服务器证书，请选择 Verify SSL。
12. 使用 shellhook 时选择 Proxy Authorization，否则清除此框。
13. 在 Additional 选项卡中，输入 HTTP Content Type。例如，application/json、application/xml 或 text/plain 代表您定义的有效负载。应用程序不会试图转换内容以匹配指定的内容类型。
14. 可选：以 JSON 提供 HTTP 标头。ERB 也被允许。

当使用非标准 HTTP 或 HTTPS 端口配置端点的 webhook 时，必须分配 SELinux 端口，请参阅从连接的网络安装 Satellite 中的自定义端口上访问 Satellite。

15.5. 可用的 WEBHOOK 事件

下表包含卫星 Web UI 中可用的 webhook 事件列表。操作 事件仅在 成功 上触发 Webhook，因此当操作失败时，不会触发 webhook。

有关有效负载的更多信息，请访问 Administer > About > Support > Templates DSL。下表提供了可用类型的列表。在这种情况下，一些事件被标记为 自定义，有效负载是一个对象，但 Ruby hash（键-值数据结构）,因此语法不同。

事件名称	描述	payload
actions Katello Content View promote Succeeded	内容视图已成功提升。	Actions::Katello::ContentView::Promote
actions Katello Content View Publish Succeeded	存储库已成功同步。	Actions::Katello::ContentView::Publish
操作远程执行运行主机作业 Succeeded	为主机成功执行通用远程执行作业。所有远程执行作业（完成后）发布此事件。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello Errata Install Succeeded	使用 Katello 接口安装勘误表。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello Group Install Succeeded	使用 Katello 接口安装 软件包组。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello Package Install Succeeded	使用 Katello 接口安装软件包。	Actions::RemoteExecution::RunHostJob
操作远程执行运行主机作业 Katello Group Remove	使用 Katello 接口删除软件包组。	Actions::RemoteExecution::RunHostJob

事件名称	描述	payload
Actions Remote Execution Run Host Job Katello Package Remove Succeeded	使用 Katello 接口删除软件包。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello Service Restart Succeeded	使用 Katello 接口重启 Services。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello Group Update Succeeded	使用 Katello 接口更新软件包组。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello Package Update Succeeded	使用 Katello 接口更新软件包。	Actions::RemoteExecution::RunHostJob
操作远程执行运行主机作业 Foreman OpenSCAP Run Scans Succeeded	运行 OpenSCAP 扫描。	Actions::RemoteExecution::RunHostJob
操作远程执行运行主机作业 Ansible Run Host Succeeded	运行一个 Ansible playbook，其中包含为主机定义的所有角色。	Actions::RemoteExecution::RunHostJob
操作远程执行运行主机作业 Ansible Run Capsule Upgrade Succeeded	在给定的胶囊服务器主机上升级胶囊。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Ansible Configure Cloud Connector Succeeded	在给定主机上配置 Cloud Connector。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Ansible Run Insights Plan Succeeded	根据一个 ID 从 Red Hat Access Insights 运行指定维护计划。	Actions::RemoteExecution::RunHostJob
操作远程执行运行主机作业 Ansible Run Playbook Succeeded	针对给定主机运行 Ansible playbook。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Ansible Enable Web Console Succeeded	运行 Ansible playbook，在给定的主机上启用 Web 控制台。	Actions::RemoteExecution::RunHostJob
操作远程执行运行主机作业 Puppet Run Host Succeeded	执行单个 Puppet 运行。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Katello module Stream Action Succeeded	使用 Katello 接口执行模块流操作。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Leapp Pre-upgrade Succeeded	RHEL 7 主机的可升级检查。	Actions::RemoteExecution::RunHostJob
Actions Remote Execution Run Host Job Leapp Remediation Plan Succeeded	使用 Leapp 运行修复计划。	Actions::RemoteExecution::RunHostJob

事件名称	描述	payload
操作远程执行运行主机作业 Leapp Upgrade Succeeded	为 RHEL 7 主机运行 Leapp 升级作业。	Actions::RemoteExecution::RunHostJob
build Entered	输入构建模式的主机。	自定义事件：@ **payload[:id]** (host id), **@payload[:hostname]** (host name)。
build Exited	主机构建模式已取消，无论它已被成功置备，或者用户手动取消了构建。	自定义事件：@ **payload[:id]** (host id), **@payload[:hostname]** (host name)。
Content View Created/Updated/Destroyed	内容视图上的常见数据库操作。	Katello::ContentView
域 Created/Updated/Destroyed	域上的常见数据库操作。	域
主机已创建/更新/介绍	主机上的通用数据库操作。	主机
主机组 Created/Updated/Destroyed	主机组上的常见数据库操作.	hostgroup
Created/Updated/Destroyed 建模	模式上的常见数据库操作。	model
status Changed	已更改主机的全局主机状态。	Custom event: **@payload[:id]** (host id), **@payload[:hostname]**, **@payload[:global_status]** (hash)
子网 Created/Updated/Destroyed	子网上的常见数据库操作。	子网
模板渲染程序执行	报告模板已呈现。	模板
用户 Created/Updated/Destroyed	用户的通用数据库操作。	User

15.6. SHELLHOOKS

*使用 **webhook** 时，一个 **Satellite** 事件只能映射到一个 **API** 调用。对于高级集成，如果单个 **shell** 脚本可以包含多个命令，您可以安装一个使用 **REST HTTP API** 来公开可执行文件的 **Capsule shellhook** 插件。*

*然后，可将 **Webhook** 配置为访问 **Capsule API** 以运行预定义的 **shellhook**，例如，可以包含命令或编辑文件。*

*脚本必须放在 **/var/lib/foreman-proxy/shellhook** 中，作为名称中只有字母数字字符和下划线的可执行文件。*

HTTPS 有效负载使用标准输入传递，可以使用 X-Shellhook-Arg-1 到 N 来提供可选的命令行参数。

HTTP 方法必须是 POST。一个 URL 示例为：
https://capsule.example.com:9090/shellhook/my_script。

您必须为每个连接到 shellhook 的 webhook 启用 代理授权，以便它能够授权调用。

标准输出和错误将分别作为带有 debug 或 warning 级别的消息重定向到胶囊日志。

没有 shellhook HTTPS 调用返回值。

15.7. 安装 SHELLHOOKS 插件

另外，您可以使用以下命令在用于 shellhook 的每个胶囊上安装并启用 shellhooks 插件：

```
# satellite-installer --enable-foreman-proxy-plugin-shellhooks
```

15.8. 使用 SHELLHOOK 参数

流程

要将参数传递给 shellhook 脚本，请创建以下 HTTP 标头：

```
{
  "X-Shellhook-Arg-1": "<%= @object.content_view_version_id %>,
  "X-Shellhook-Arg-2": "<%= @object.content_view_name %>
}
```

确保内容呈现到有效的 JSON。此外，仅传递安全字段，如数据库 ID、名称或标签，它们不包括新行或带引号字符。

第 16 章 搜索和书签

卫星 Web UI 具有强大的搜索功能，可在大多数 Web UI 页面上使用。它可让您搜索卫星服务器管理的所有资源。可搜索免费文本和基于语法的查询，可以使用广泛的输入预测进行构建。可将搜索查询保存为书签，供以后重复使用。

16.1. 构建搜索查询

当您开始输入搜索查询时，会出现完成查询当前部分的有效选项列表。您可以从列表中选择一个选项，并使用预测来保持查询，或者继续键入。要了解搜索引擎如何解释免费文本，请参阅 第 16.2 节 “使用可用文本搜索”。

16.1.1. 查询语法

```
parameter operator value
```

可用的字段、搜索资源以及查询的解释方式取决于上下文，即执行搜索的页面。例如，Hosts 页面上的"hostgroup"字段等同于 Host Groups 页面中的字段"name"。字段类型也决定可用的操作器和接受值。如需所有 Operator 的列表，请参阅 Operator。有关值格式的描述，请参阅 值。

16.1.2. Operator

下表中列出了可在 参数和值 之间使用的所有运算符。可能出现在预测构建的查询（如冒号）中的其他符号和特殊字符（如冒号）没有特殊含义，并被视为空闲文本。

表 16.1. 搜索接受的 Operator 比较

Operator	短名称	描述	示例
=	等于	接受数字、临时或文本值。对于文本，将返回确切的区分大小写匹配项。	**hostgroup = RHEL7**
!=	不等于		
~	就像	接受文本或临时值。返回不区分大小写的匹配项.接受以下通配符：_ 表示单个字符，% 或 * 代表任意数量的字符，包括零。如果没有指定通配符，则字符串将被视为在通配符中由通配符： %rhel7%	**hostgroup ~ rhel%**
!~	不喜欢		
>	大于	接受数字或时序值。对于 temporal 值，Operator > 解释为 "later than"，< 为 "earlier than"。两个运算符都可以与 EQUALS: >= <=合并。	**registered_at > 10-January-2017** **搜索将返回在给定日期后注册的主机，即 2017 年 1 月 10 日和现在之间注册的主机。** **registered_at <= Yesterday** 搜索将返回已注册 yesterday 或更早版本的主机。
<	小于		

Operator	短名称	描述	示例
^	IN	将表达式与值列表进行比较，如 SQL 中。返回包含或不分别包含值的匹配项。	**release_version !^ 7**
!^	不在		
HAS 或设置？		返回存在或不存在的值。	在 Puppet 类页面上 **有 hostgroup** 或 **set? hostgroup**，搜索将返回分配给至少一个主机组的类。 在带有主机概述的 Dashboard 上没有 **hostgroup** 或 **null? hostgroup**，搜索将返回没有分配主机组的所有主机。
不是 HAS 或 null？			

遵循上述语法的简单查询可以通过逻辑运算符 AND、OR 和 not 合并到更复杂的域中。还可接受 Operator 的替代表示法：

表 16.2. 搜索接受的逻辑 Operator

Operator	其它通知			示例
和	&	&&	<whitespace>	类 = motd AND 环境 ~ 生产
或者	|	||		**errata_status = errata_needed || errata_status = security_needed**
not	–	!		**hostgroup ~ rhel7 not status.failed**

16.1.3. 值

文本值

包含空格的文本必须用引号括起。否则，空格被解释为 AND 运算符。
示例：

hostgroup = "Web 服务器"

搜索将返回名为"Web servers"的已分配主机组的主机。

hostgroup = Web 服务器

搜索将返回主机组 Web 中的主机，并且任何匹配 %servers% 的字段。

临时值

接受很多日期和时间格式，包括：

- *"2017 年 1 月 10 日"*

- "2017 年 1 月 10 日"
- 10-January-2017
- 10/January/2017
- "January 10, 2017 年"
- 目前，是的，

警告

避免模糊日期格式，如 02/10/2017 或 10-02-2017。

16.2. 使用可用文本搜索

当您输入空闲文本时，将搜索到多个字段。例如，如果您输入"64"，则搜索将返回名称、IP 地址、MAC 地址和架构中包含该数字的所有主机。

注意

多词语查询必须以引号括起，否则空格被解释为 AND 运算符。

由于在所有字段间搜索，免费文本搜索结果不准确，且搜索可能会很慢，特别是在大量主机上。因此，我们建议您避免免费文本，并尽可能使用更具体的、基于语法的查询。

16.3. 管理书签

您可以将搜索查询保存为用于重复使用的书签。您还可以删除或修改书签。

书签仅显示在创建它们的页面上。在一些页面中，还有可用于常用搜索的默认书签，例如，所有 活跃 或 禁用 的主机。

16.3.1. 创建书签

本节详细介绍了如何将搜索查询保存为书签。您必须在相关页面中保存搜索查询，为该页面创建书签，例如，在 Hosts 页面上保存主机相关搜索查询。

要创建书签：

1. 导航到您要创建书签的页面。
2. 在 Search 字段中输入您要保存的搜索查询。
3. 选择搜索按钮右侧的箭头，然后选择 此搜索标记。
4. 在 Name 字段中输入新书签的名称。

5. 在 Search query 字段中，确保搜索查询正确。
6. 确保正确设置公共复选框 ：
   - 选择 公共复选框，将书签设置为公共，并对所有用户可见。
   - 清除 公共复选框，将书签设置为私有，且仅对创建它的用户可见。
7. 点 Submit。

要确认创建，请选择 Search 按钮右侧的箭头，以显示书签列表，或者导航到 Administer > Bookmarks，然后选中该书签名称的书签列表。

16.3.2. 删除书签

您可以在 "书签" 页面中删除书签。

要删除书签：

1. 导航到 Administer > Bookmarks。
2. 在 Bookmarks 页面上，单击 Delete 作为您要删除的书签。
3. 确认窗口打开后，单击确定以确认 删除。

要确认删除，请选中 书签名称中的书签列表。

附录 A. SATELLITE 设置

*本节包含在 **Satellite Web UI** 中编辑的设置的信息或已知问题，具体操作为：导航到 **Administer > Settings**。*

表 A.1. 常规设置信息

设置	描述
修复 DB 缓存	Satellite 维护权限和角色的缓存。当设置为 **Yes** 时，Satellite 会在下一次重启时重新创建这个缓存。

表 A.2. 置备设置信息

设置	描述
名称生成器类型	指定在创建新主机时用于生成主机名的方法。 **基于默认 Random 的** 选项会生成一个唯一的随机主机名，但不必使用它们。这对创建多个主机并不知道如何命名主机的用户很有用。 **基于 MAC** 的 选项仅适用于裸机主机。如果您删除主机并在以后创建它，它将根据 MAC 地址接收相同的主机名。这对回收服务器的用户来说非常有用，希望他们始终获得相同的主机名。 **Off** 选项禁用名称生成器函数，并将主机名字段留空。
Safemode rendering	启用置备模板的安全模式渲染。默认和推荐的选项是拒绝对变量的访问以及没有在 Satellite 中列入的任何对象。 **当设置为 No 时，用户可通过编辑模板、参数或智能变量的权限访问任何对象。这允许用户在卫星服务器上完全执行远程代码，从而有效地禁用所有授权。这不是一种安全选择，特别是在大型公司中。**
存储在 Satellite 中的事实的排除模式	在 BZ#1759111 被解决前，请注意，如果您使用通配符值（如 **docker** *）来排除以 **docker** 开头的所有事实，这也会排除在名称中的任何部分包含排除术语的事实。

设置	描述
忽略具有匹配标识符的接口	在 BZ#1759111 被解决前，请注意，如果您使用通配符值，如 **docker***，忽略以 **docker** 开头的所有事实，这也会排除在名称中的任何部分包含被忽略术语的事实。