



Red Hat Satellite 6.12

管理 Red Hat Satellite

管理红帽卫星的指南。

Red Hat Satellite 6.12 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

Copyright © 2024 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

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

向红帽文档提供反馈	5
第 1 章 访问 RED HAT SATELLITE	6
1.1. 导入 KATELLO ROOT CA 证书	6
1.2. 登录到 SATELLITE	6
1.3. 在卫星 WEB UI 中导航标签	7
1.4. 更改密码	7
1.5. 重置管理用户密码	8
1.6. 在登录页面中设置自定义消息	8
第 2 章 启动和停止 RED HAT SATELLITE	9
第 3 章 从内部 SATELLITE 数据库迁移到外部数据库	10
3.1. POSTGRESQL 作为外部数据库注意事项	10
3.2. 为外部数据库准备主机	11
3.3. 安装 POSTGRESQL	11
3.4. 迁移到外部数据库	13
第 4 章 使用 ANSIBLE COLLECTIONS 管理 SATELLITE	15
4.1. 安装 SATELLITE ANSIBLE 模块	15
4.2. 查看 SATELLITE ANSIBLE 模块	15
第 5 章 管理机构	16
5.1. 创建机构	16
5.2. 设置机构上下文	17
5.3. 创建机构调试证书	17
5.4. 使用机构调试证书浏览存储库内容	17
5.5. 删除机构	18
第 6 章 管理位置	20
6.1. 创建位置	20
6.2. 创建多个位置	20
6.3. 设置位置上下文	21
6.4. 删除位置	21
第 7 章 管理用户和角色	22
7.1. 管理用户	22
7.2. 管理 SSH 密钥	24
7.3. 管理个人访问令牌	26
7.4. 创建和管理用户组	27
7.5. 创建和管理角色	28
7.6. SATELLITE 中可用的预定义角色	31
7.7. 细粒度权限过滤	32
第 8 章 配置电子邮件通知	36
8.1. 电子邮件通知类型	36
8.2. 配置电子邮件通知首选项	36
8.3. 测试电子邮件发送	37
8.4. 测试电子邮件通知	37
8.5. 更改主机的电子邮件通知设置	38
第 9 章 管理安全合规性	39
9.1. 安全内容自动化协议	39
9.2. SATELLITE 中的 SCAP 内容	39

9.3. 合规策略部署选项	40
9.4. 配置合规策略部署方法	40
9.5. 列出可用的 SCAP 内容	41
9.6. 配置 SCAP 内容	41
9.7. 管理合规策略	44
9.8. 部署合规策略	46
9.9. 对需求运行安全合规扫描	49
9.10. 监控合规性	50
第 10 章 备份 SATELLITE 服务器和胶囊服务器	54
10.1. 估算备份的大小	54
10.2. 执行 SATELLITE 服务器或 CAPSULE SERVER 的完整备份	55
10.3. 执行没有 PULP 内容的备份	57
10.4. 执行增量备份	57
10.5. WEEKLY FULL BACKUP FOLLOWED BY DAILY INCREMENTAL BACKUPS 示例	58
10.6. 执行在线备份	58
10.7. 执行快照备份	59
10.8. 在执行备份时列出和跳过步骤	60
第 11 章 从备份中恢复 SATELLITE 服务器或胶囊服务器	61
11.1. 从完整备份中恢复	61
11.2. 从增量备份中恢复	62
11.3. 使用虚拟机快照备份和恢复胶囊服务器	62
第 12 章 重命名 SATELLITE SERVER 或 CAPSULE SERVER	63
12.1. 重命名卫星服务器	63
12.2. 重命名胶囊服务器	64
第 13 章 维护 SATELLITE 服务器	67
13.1. 删除审计记录	67
13.2. 匿名审计记录	67
13.3. 删除 REPORT RECORDS	67
13.4. 配置 CLEANING UNUSED TASKS 功能	68
13.5. 删除任务记录	69
13.6. 按 ID 删除任务	69
13.7. 从完整磁盘中恢复	70
13.8. 在卫星服务器或胶囊服务器基本操作系统上管理软件包	71
13.9. 重新声明 POSTGRESQL 空间	72
第 14 章 续订自定义 SSL 证书	74
14.1. 在 SATELLITE 服务器上续订自定义 SSL 证书	74
14.2. 在 CAPSULE 服务器上续订自定义 SSL 证书	75
第 15 章 日志记录和报告问题	77
15.1. 启用调试日志记录	77
15.2. 通过调试增加日志记录级别	77
15.3. 检索服务的状态	84
15.4. 重启服务	85
15.5. 启用单个日志记录器	85
15.6. 配置日志记录到日志或基于文件的日志记录	87
15.7. SATELLITE 提供的日志文件目录	88
15.8. COLLECTING 日志信息的工具	88
15.9. 系统日志元数据	89
第 16 章 监控资源	91

16.1. 使用 RED HAT SATELLITE CONTENT DASHBOARD	91
16.2. 配置 RSS 通知	96
16.3. 监控 SATELLITE 服务器	96
16.4. 监控胶囊服务器	97
第 17 章 使用 WEBHOOK	99
17.1. 迁移到 WEBHOOK	100
17.2. 安装 WEBHOOK	100
17.3. 创建 WEBHOOK 模板	100
17.4. 创建 WEBHOOK	101
17.5. 可用的 WEBHOOK 事件	103
17.6. SHELLHOOKS	105
17.7. 安装 SHELLHOOKS 插件	106
17.8. 使用 WEBHOOK 将参数传递给 SHELLHOOK 脚本	106
17.9. 使用 CURL 将参数传递给 SHELLHOOK 脚本	107
17.10. 创建 SHELLHOOK 以打印参数	108
第 18 章 搜索和书签	111
18.1. 构建搜索查询	111
18.2. 使用可用文本搜索	114
18.3. 管理书签	114
附录 A. 管理设置	117
A.1. 常规设置	117
A.2. SATELLITE 任务设置	118
A.3. 模板同步设置	119
A.4. 发现的设置	120
A.5. 引导磁盘设置	121
A.6. RED HAT CLOUD SETTINGS	122
A.7. 内容设置	122
A.8. 身份验证设置	126
A.9. 电子邮件设置	128
A.10. 通知设置	129
A.11. 置备设置	129
A.12. 事实设置	132
A.13. 配置管理设置	133
A.14. 远程执行设置	133
A.15. ANSIBLE 设置	135

向红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。

您可以通过在 Bugzilla 中记录一个 ticket 来提交反馈：

1. 导航到 [Bugzilla](#) 网站。
2. 在 **Component** 字段中，使用 **Documentation**。
3. 在 **Description** 字段中，输入您要改进的建议。包括文档相关部分的链接。
4. 点 **Submit Bug**。

第 1 章 访问 RED HAT SATELLITE

在安装并配置 Red Hat Satellite 后，使用 Satellite Web UI 界面登录 Satellite 以进行进一步配置。

1.1. 导入 KATELLO ROOT CA 证书

第一次登录 Satellite 时，您可能会看到一个警告，通知您正在使用默认自签名证书，并且您可能无法在浏览器中导入 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，并将其导入到您的浏览器中。

要使用 CLI 而不是 Satellite Web UI，请参阅 [CLI 过程](#)。

前提条件

- 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。

CLI 过程

1. 在 Satellite CLI 中，将 **katello-server-ca.crt** 文件复制到用于访问 Satellite 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 用户界面登录卫星，以进行进一步配置。

前提条件

- 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“导入 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`。如果您登录时，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。

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 <i>Any Organization</i> ，默认位置为 <i>Any Location</i> 。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	提供配置卫星如何与环境交互的工具。
用户名	为用户管理，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。

流程

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。

- 点 **Submit** 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

- 登录到安装了 Satellite 服务器的基本操作系统。
- 输入以下命令重置密码：

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

- 使用此密码在卫星 Web UI 中重置密码。
- 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

- 登录到安装了 Satellite 服务器的基本操作系统。
- 要设置密码，请输入以下命令：

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

- 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

流程

- 在 Satellite Web UI 中，导航到 **Administer > Settings**，然后点 **General** 选项卡。
- 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。
- 点击 **Save**。
- 从卫星 Web UI 注销，并验证自定义文本现在显示在 Satellite 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 10 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 服务，请执行：

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

要启动 Satellite 服务，请执行：

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

要重启 Satellite 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 8 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。

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 8 安装一个最新置备的系统，以托管外部数据库。

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。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。

前提条件

- 准备好的主机必须满足卫星 [的存储要求](#)。

流程

1. 使用 [Attaching Satellite Infrastructure Subscription](#) 中的说明将 Satellite 订阅附加到您的服务器。
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=satellite-6.12-for-rhel-8-x86_64-rpms \
--enable=rhel-8-for-x86_64-baseos-rpms \
--enable=rhel-8-for-x86_64-appstream-rpms
```

3. 启用以下模块：

```
# dnf module enable satellite:el8
```



注意

启用模块 **satellite:el8** 会警告与 **postgresql:10** 和 **ruby:2.5** 冲突，因为这些模块在 Red Hat Enterprise Linux 8 中被设置为默认模块版本。模块 **satellite:el8** 依赖于模块 **postgresql:12** 和 **ruby:2.7**，它将通过 **satellite:el8** 模块启用。这些警告不会导致安装过程失败，因此可以安全地忽略。有关 Red Hat Enterprise Linux 8 中的模块和生命周期流的更多信息，请参阅 [Red Hat Enterprise Linux Application Streams 生命周期](#)。

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。Satellite 支持 PostgreSQL 版本 12。

流程

1. 要安装 PostgreSQL，请输入以下命令：

```
# dnf install postgresql-server postgresql-evr
```

2. 要初始化 PostgreSQL，请输入以下命令：

```
# postgresql-setup initdb
```

3. 编辑 `/var/lib/pgsql/data/postgresql.conf` 文件：

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

请注意，需要调整外部 PostgreSQL 的默认配置，以便使用 Satellite。推荐的外部数据库配置调整基本如下：

- checkpoint_completion_target: 0.9
- max_connections: 500
- shared_buffers: 512MB
- work_mem: 4MB

4. 删除 # 并编辑 以侦听入站连接：

```
listen_addresses = '*'
```

5. 编辑 `/var/lib/pgsql/data/pg_hba.conf` 文件：

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

6. 在文件中添加以下行：

```
host all all Satellite_ip/32 md5
```

7. 要启动并启用 PostgreSQL 服务，请输入以下命令：

```
# systemctl enable --now 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。

前提条件

- 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 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 \
  --foreman-db-username foreman \
  --katello-candlepin-db-host postgres.example.com \
  --katello-candlepin-db-name candlepin \
  --katello-candlepin-db-password Candlepin_Password \
  --katello-candlepin-manage-db false \
  --katello-candlepin-db-user candlepin \
```

```
--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 \  
--foreman-proxy-content-pulpcore-postgresql-user pulp
```

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. 安装 SATELLITE ANSIBLE 模块

使用此流程安装 Satellite Ansible 模块。

流程

- 使用以下命令安装软件包：

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

4.2. 查看 SATELLITE ANSIBLE 模块

您可以运行以下命令来查看已安装的 Satellite Ansible 模块：

```
# ansible-doc -l redhat.satellite
```

另外，您还可以在 [Red Hat Ansible Automation Platform](#) 中看到 Satellite Ansible 模块的完整列表和其他相关信息。

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 管理机构

组织根据所有权、目的、内容、安全级别或其他部门将红帽卫星资源划分为逻辑组。您可以通过 Red Hat Satellite 创建和管理多个组织，然后将您的红帽订阅划分并分配给每个单独的组织。这提供了一种管理单一管理系统下多个组织的内容的方法。以下是机构管理的一些示例：

单个机构

具有简单系统管理链的小型企业。在这种情况下，您可以为业务创建一个组织，并为它分配内容。

多机构

拥有多个较小业务部门的大型公司。例如，拥有单独的系统管理和软件开发组的公司。在这种情况下，您可以为公司及其拥有的每个业务部门创建组织。这会为每个独立的系统基础架构保持系统基础架构。然后，您可以根据每个组织的需求将内容分配给每个组织。

外部机构

家为其他企业管理外部系统的公司。例如，公司向客户提供云计算和 Web 托管资源。在这种情况下，您可以为公司自己的系统基础架构创建一个机构，然后为每个外部业务创建一个组织。然后，您可以根据需要为每个机构分配内容。

Red Hat Satellite 的默认安装中有一个名为 **Default Organization** 的默认机构。

新用户

如果没有为新用户分配默认机构，则访问会被限制。要为用户授予系统权利，请将它们分配给默认机构。当用户下次登录到 Satellite 时，用户帐户具有正确的系统权限。

5.1. 创建机构

使用此流程创建机构。要使用 CLI 而不是 Satellite Web UI，请参阅 [CLI 过程](#)。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Organizations**。
2. 单击**新建组织**。
3. 在 **Name** 字段中输入机构的名称。
4. 在 **Label** 字段中输入机构的唯一标识符。这用于创建和映射某些资产，如内容存储的目录。使用字母、数字、下划线和短划线，但没有空格。
5. 可选：在 **Description** 字段中输入机构的描述。
6. 点 **Submit**。
7. 如果您没有分配机构的主机，请选择您要添加到机构中的主机，然后单击 **Proceed to Edit**。
8. 在 **Edit** 页面中，分配您要添加到机构的基础架构资源。这包括网络资源、安装介质、Kickstart 模板和其他参数。您可以随时导航到 **Administer > Organizations**，然后选择一个机构进行编辑。
9. 点 **Submit**。

CLI 过程

1. 运行以下命令来创建机构：

```
# hammer organization create \
--name "My_Organization" \
--label "My_Organization_Label" \
--description "My_Organization_Description"
```

2. 可选：要编辑机构，请输入 **hammer 机构更新** 命令。例如，以下命令将计算资源分配给机构：

```
# hammer organization update \
--name "My_Organization" \
--compute-resource-ids 1
```

5.2. 设置机构上下文

组织上下文定义了要用于主机及其相关资源的组织。

流程

组织菜单是卫星 Web UI 左上菜单栏中的第一个菜单项。如果您尚未选择当前组织，则菜单显示 **任何组织**。单击 **Any Organization** 按钮，再选择要使用的组织。

CLI 过程

使用 CLI 时，将 **--organization "My_Organization"** 或 **--organization-label "My_Organization_Label"** 作为选项。例如：

```
# hammer subscription list \
--organization "My_Organization"
```

此命令输出为 *My_Organization* 分配的订阅。

5.3. 创建机构调试证书

如果需要您的机构 debug 证书，请使用以下步骤。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Organizations**。
2. 选择您要为其生成 debug 证书的机构。
3. 点 **Generate and Download**。
4. 将证书文件保存在安全位置。

为调配模板调试证书

如果置备模板下载，则会自动生成调试证书下载它们。

5.4. 使用机构调试证书浏览存储库内容

如果使用 Web 浏览器或具有该组织的调试证书，您可以使用 Web 浏览器或 API 查看机构的存储库内容。

前提条件

- 您创建并下载了组织证书。更多信息请参阅 [第 5.3 节 “创建机构调试证书”](#)。

流程

1. 将私钥和公钥从证书分成两个文件。

- a. 为默认机构打开 X.509 证书：

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

- b. 将 `-----BEGIN RSA PRIVATE KEY-----` 中的文件内容复制到 `-----END RSA PRIVATE KEY-----` 中，再把一个 `key.pem` 文件复制到 `key.pem` 文件中。
- c. 将 `-----BEGIN CERTIFICATE-----` 的内容复制到 `-----END CERTIFICATE-----` 中，再把 `-----BEGIN CERTIFICATE-----` 复制到 `cert.pem` 文件中。

2. 要使用浏览器，您必须首先将 X.509 证书转换为浏览器支持并导入证书的格式。

对于 Firefox 用户

1. 使用以下命令将证书转换为 PKCS12 格式：

```
$ openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in cert.pem -inkey key.pem -out My_Organization_Label.pfx -name My_Organization
```

2. 在 Firefox 浏览器中，导航到 **Edit > Preferences > Advanced Tab**。
3. 选择 "查看证书" 并单击 "证书" 选项卡。
4. 单击 **Import**，再选择要加载的 `.pfx` 文件。
5. 在地址栏中输入以下 URL 来浏览所有仓库的可访问路径并检查其内容：

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

对于 CURL 用户

- 要在 CURL 中使用机构 debug 证书，请输入以下命令：

```
$ curl -k --cert cert.pem --key key.pem \
https://satellite.example.com/pulp/content/My_Organization_Label/Library/content/dist/rhel/server/7/7Server/x86_64/os/
```

确保到 `cert.pem` 和 `key.pem` 的路径是正确的绝对路径，否则命令会以静默方式失败。Pulp 使用组织标签，因此您必须在 URL 中输入组织标签。

5.5. 删除机构

如果组织没有与任何生命周期环境或主机组关联，您可以删除机构。如果存在与您要删除的机构关联的任何生命周期环境或主机组，请导航到 **Administer > Organizations** 并点相关的机构来删除它们。不要删除安装期间创建的默认组织，因为默认组织是卫星环境中任何未关联主机的占位符。在任何给定时间，环境中必须至少有一个机构。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Organizations**。
2. 从您要删除的机构名称右侧的列表中，选择 **Delete**。
3. 单击 **OK** 以删除该组织。

CLI 过程

1. 输入以下命令检索您要删除的机构 ID：

```
# hammer organization list
```

在输出中，记录您要删除的机构的 ID。

2. 输入以下命令删除机构：

```
# hammer organization delete --id Organization_ID
```

第 6 章 管理位置

位置功能与机构类似：它们提供了一种对资源进行分组和分配主机的方法。组织和位置有以下概念差异：

- 位置基于物理或虚拟地理设置。
- 位置具有层次结构。

6.1. 创建位置

使用此流程创建位置，以便您可以按照位置管理主机和资源。要使用 CLI 而不是 Satellite Web UI，请参阅 [CLI 过程](#)。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Locations**。
2. 单击 **New Location**。
3. 可选：从 **Parent** 列表选择一个父位置。这会创建位置层次结构。
4. 在 **Name** 字段中输入位置的名称。
5. 可选：在 **Description** 字段中输入位置的描述。
6. 点 **Submit**。
7. 如果您的主机没有分配位置，请添加您要分配给新位置的任何主机，然后单击 **Proceed to Edit**。
8. 分配您要添加到位置的任何基础架构资源。这包括网络资源、安装介质、Kickstart 模板和其他参数。您可以随时通过导航到 **Administer > Locations**，然后选择要编辑的位置来返回到此页面。
9. 点 **Submit** 保存您的更改。

CLI 过程

- 输入以下命令来创建位置：

```
# hammer location create \  
--description "My_Location_Description" \  
--name "My_Location" \  
--parent-id "My_Location_Parent_ID"
```

6.2. 创建多个位置

以下示例 Bash 脚本会创建三个位置 - 伦敦、慕尼黑、波士顿，并将它们分配到 Example 组织。

```
ORG="Example Organization"  
LOCATIONS="London Munich Boston"  
  
for LOC in ${LOCATIONS}  
do
```



```
hammer location create --name "${LOC}"
hammer location add-organization --name "${LOC}" --organization "${ORG}"
done
```

6.3. 设置位置上下文

位置上下文定义了用于主机及其相关资源的位置。

流程

位置菜单是菜单栏上的第二个菜单项，它位于卫星 Web UI 左侧。如果您尚未选择当前位置，菜单将显示 **Any Location**。单击 **Any 位置**，再选择要使用的位置。

CLI 过程

使用 CLI 时，将 `--location "My_Location"` 或 `--location-id "My_Location_ID"` 包含作为选项。例如：

```
# hammer host list --location "My_Location"
```

此命令列出与 `My_Location` 位置关联的主机。

6.4. 删除位置

如果该位置没有与任何生命周期环境或主机组关联，您可以删除该位置。如果有任何生命周期环境或与您要删除的位置关联的主机组，请导航到 **Administer > Locations** 并点相关的位置来删除它们。不要删除安装期间创建的默认位置，因为默认位置是卫星环境中任何未关联主机的占位符。在任何给定时间，环境中必须至少有一个位置。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Locations**。
2. 从您要删除的位置名称右侧的列表中选择 **Delete**。
3. 单击 **OK** 以删除该位置。

CLI 过程

1. 输入以下命令检索您要删除的位置的 ID：

```
# hammer location list
```

在输出中，记下您要删除的位置的 ID。

2. 输入以下命令删除位置：

```
# hammer location delete --id Location ID
```

第 7 章 管理用户和角色

用户为使用系统的个人定义了一组详细信息。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 7.1 节“管理用户”](#)。

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 7.4 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** 进行了分组。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。Satellite 提供一组预定义的角色，还可创建自定义角色和权限过滤器，如 [第 7.5 节“创建和管理角色”](#) 所述。

7.1. 管理用户

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。

7.1.1. 创建用户

使用此流程创建用户。要使用 CLI 而不是 Satellite Web UI，请参阅 [CLI 过程](#)。

流程

1. 在 Satellite Web UI 中，导航到 **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 [在连接的网络环境中安装卫星服务器中的配置外部身份验证](#) 中所述。
 - 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 \
--auth-source-id My_Authentication_Source \
--login My_User_Name \
--mail My_User_Mail \
--organization-ids My_Organization_ID_1,My_Organization_ID_2 \
--password My_User_Password
```

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**。

7.1.2. 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 Satellite Web UI，请参阅 [CLI 过程](#)。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Users**。
2. 单击要分配给一个或多个角色的用户的 **username**。



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，可选择 **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
```

7.1.3. 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

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。

7.1.4. 创建仅限 API 的用户

您可以创建只与 Satellite API 交互的用户。

前提条件

- 您已创建了用户并为其分配角色。请注意，此用户必须在内部授权。如需更多信息，请参阅 [创建用户并为用户分配角色](#)。

流程

1. 以 admin 用户身份登录您的 Satellite。
2. 导航到 **Administer > Users** 并选择一个用户。
3. 在 **User** 选项卡中，设置密码。请勿保存或与他人沟通。您可以在控制台中创建伪随机字符串：

```
# openssl rand -hex 32
```

4. 为用户创建个人访问令牌。如需更多信息，请参阅 [第 7.3.1 节“创建个人访问令牌”](#)。

7.2. 管理 SSH 密钥

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 密钥的详情，请参考在置备 [主机过程中部署 SSH 密钥](#)。

有关 SSH 密钥和 SSH 密钥创建的详情，请参考在 *Red Hat Enterprise Linux 8 配置基本系统设置* 中的 [使用基于 SSH 的身份验证](#)。

7.2.1. 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 Satellite Web UI，请参阅 [CLI 过程](#)。

先决条件

- 确保您以 Red Hat Satellite 的 Admin 用户身份或为添加 SSH 密钥启用了 `create_ssh_key` 权限，为删除密钥启用了 `destroy_ssh_key` 权限的用户身份登陆到 Satellite web UI，用于。

流程

1. 在 Satellite Web UI 中，导航到 **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 1/46MTIZo9CPTX4CYUHeN8=
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
```

7.3. 管理个人访问令牌

个人访问令牌允许您在不使用密码的情况下验证 API 请求。您可以为个人访问令牌设置过期日期，如果您决定应在过期日期前过期，可以撤销它。

7.3.1. 创建个人访问令牌

使用这个流程创建个人访问令牌。

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Users**。
2. 选择您要为其创建个人访问令牌的用户。
3. 在 **Personal Access Tokens** 选项卡中，点 **Add Personal Access Token**。
4. 输入个人访问令牌的名称。
5. 可选：选择 **过期日期** 来设置过期日期。如果您没有设置过期日期，您的个人访问令牌将永远不会过期，除非撤销。
6. 点 **Submit**。现在，您已在个人访问令牌 选项卡中有个人访问令牌。



重要

确存储您的个人访问令牌，因为您将无法在页面离开或创建新的个人访问令牌后再次访问它。您可以点击 **Copy to clipboard** 复制个人访问令牌。

验证

1. 向 Satellite 服务器发出 API 请求，并使用您的个人访问令牌进行身份验证：

```
# curl https://satellite.example.com/api/status --user  
My_Username:My_Personal_Access_Token
```

2. 您应该收到状态为 **200** 的响应，例如：

```
{"satellite_version":"6.12.0","result":"ok","status":200,"version":"3.5.1.10","api_version":2}
```

如果您返回 **个人访问令牌** 选项卡，您可以看到个人访问令牌旁的更新的 **Last Used** 时间。

7.3.2. 撤销个人访问令牌

使用这个流程在过期日期前撤销个人访问令牌。

流程

1. 在 Satellite Web UI 中，导航到 Administer >Users。
2. 选择您要撤销个人访问令牌的用户。
3. 在个人访问令牌选项卡中，找到您要撤销的个人访问令牌。
4. 在您要撤销的个人访问令牌旁边的 Actions 列中点 Revoke。

验证

1. 向 Satellite 服务器发出 API 请求，并尝试使用撤销的个人访问令牌进行身份验证：

```
# curl https://satellite.example.com/api/status --user
My_Username:My_Personal_Access-Token
```

2. 您会收到以下出错信息：

```
{
  "error": {"message":"Unable to authenticate user My_Username"}
}
```

7.4. 创建和管理用户组

7.4.1. 用户组

使用 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，如在[连接的网络环境中安装 Satellite 服务器](#)中[配置外部用户组](#)中所述。

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。

7.4.2. 创建用户组

使用此[流程](#)来创建用户组。

流程

1. 在 Satellite Web UI 中，导航到 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 My_User_Group_Name \  
--role-ids My_Role_ID_1,My_Role_ID_2 \  
--user-ids My_User_ID_1,My_User_ID_2
```

7.4.3. 删除用户组

使用卫星 Web UI 删除用户组。

流程

1. 在 Satellite Web UI 中，导航到 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。

7.5. 创建和管理角色

Satellite 提供了一组对标准任务具有足够权限的预定义角色，如 [第 7.6 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。

7.5.1. 创建角色

使用此流程创建角色。

流程

1. 在 Satellite Web UI 中，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 My_Role_Name
```

为满足其目的，角色必须包含权限。创建角色后，进入 [第 7.5.3 节 “为角色添加权限”](#)。

7.5.2. 克隆角色

使用卫星 Web UI 克隆角色。

流程

1. 在 Satellite Web UI 中，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。

7.5.3. 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 Satellite Web UI，请参阅 [CLI 过程](#)。

流程

1. 在 Satellite Web UI 中，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 无限 和 覆盖 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 无限 复选框时，搜索字段 将激活。在此字段中，您可以使用 Satellite 搜索语法指定进一步过滤。更多信息请参阅 [第 7.7 节“细粒度权限过滤”](#)。启用 覆盖 复选框时，您可以添加额外位置和机构，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 \  
--permission-ids My_Permission_ID_1,My_Permission_ID_2\  
--role My_Role_Name
```

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。

7.5.4. 查看角色的权限

使用卫星 Web UI 查看角色的权限。

流程

1. 在 Satellite Web UI 中，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。更多信息请参阅 [第 7.5.5 节“创建完全权限表”](#)。

7.5.5. 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。

7.5.6. 删除角色

使用卫星 Web UI 删除角色。

流程

1. 在 Satellite Web UI 中，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。

7.6. SATELLITE 中可用的预定义角色

下表提供了 Satellite 中预定义角色授予用户的权限概述。

要查看预定义角色授予的确切权限集，请以特权用户身份在 Satellite Web UI 中显示角色。如需更多信息，请参阅 [第 7.5.4 节“查看角色的权限”](#)。

表 7.1. 角色提供的权限

角色	角色提供的权限
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。
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。

角色	角色提供的权限
编辑分区表	查看、创建、编辑和销毁分区表。
Manager (管理者)	查看并编辑全局设置。
机构管理员	除管理机构的权限外的所有权限。 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。 通过克隆此角色并分配机构，您可以将该机构的管理委托给用户。
红帽访问日志	查看日志查看器和日志。
远程执行管理器	控制哪些角色有权运行基础架构作业。
远程执行用户	针对主机运行远程执行作业。
网站管理器	Manager 角色的约束版本。
系统管理员	<ul style="list-style-type: none"> 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。 <p>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。</p>
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。

7.7. 细粒度权限过滤

如第 7.5.3 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。

7.7.1. 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 Satellite 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。取消选择字段的无限复选框，使其处于活跃状态。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。如需了解适用的操作符的概述信息，请参阅 [第 7.7.3 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 `and`，`not`和`has`）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。

7.7.2. 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。

7.7.2.1. 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`、`Yyyyy` 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，有些资源类型提供了 GUI 替代方案，一个提供了 Locations 和 Organizations 选项卡的 Override 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。更多信息请参阅 [第 7.7.2.2 节“创建机构特定管理器角色”](#)。

7.7.2.2. 创建机构特定管理器角色

使用卫星 Web UI 创建仅限于名为 *org-1* 的单一组织的管理角色。

流程

1. 在 Satellite Web UI 中，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 and 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。

7.7.3. Granular Search 支持的 Operator

表 7.2. 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 7.3. 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 8 章 配置电子邮件通知

电子邮件通知由卫星服务器定期创建，或者在完成某些事件后创建。定期通知每天、每周或每月发送。

有关可用通知类型的概述，请参阅 [第 8.1 节 “电子邮件通知类型”](#)。

用户默认不收到任何电子邮件通知。管理员可以根据通知类型以及频率等标准，将用户配置为接收通知。



重要

默认情况下，卫星服务器不启用传出电子邮件，因此您必须查看您的电子邮件。有关更多信息，请参阅 [在连接的网络环境中安装 Satellite 服务器中的为传出电子邮件配置 Satellite 服务器](#)。

8.1. 电子邮件通知类型

Satellite 可以创建以下电子邮件通知：

- **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。
- **合规策略摘要**：OpenSCAP 策略报告概述及其结果。
- **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。
- **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。

如需电子邮件通知类型的完整列表，请导航到 Satellite Web UI 中的 Administer > Users，点所需用户的 Username，然后选择 Email Preferences 选项卡。

8.2. 配置电子邮件通知首选项

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。



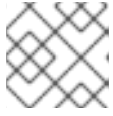
注意

如果要将在电子邮件通知发送到组电子邮件地址而不是单独的电子邮件地址，请创建一个具有组电子邮件地址、最小 Satellite 权限的用户帐户，然后将用户帐户订阅到所需的 notification 类型。

流程

1. 在 Satellite Web UI 中，导航到 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。

8.3. 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。

8.4. 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:_My_Frequency_
```

将 *My_Frequency* 替换为以下之一:

- 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。

8.5. 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。

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。

流程

1. 在 Satellite Web UI 中，进入到 Hosts > All Hosts，找到您要查看的主机，并在 Actions 列中点击 Edit。
2. 进入 Additional Information 选项卡。如果选中了在 Satellite 报告中包含此主机的复选框，则会在该主机上启用电子邮件通知。
3. 可选：切换复选框以启用或禁用电子邮件通知。



注意

如果要接收电子邮件通知，请确保在用户设置中设置了电子邮件地址。

第 9 章 管理安全合规性

安全合规管理是定义安全策略的持续流程，审计系统符合这些政策，并解决不合规实例。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。

使用 Satellite，您可以在所有注册的主机上调度合规审计和报告。

9.1. 安全内容自动化协议

Satellite 使用安全内容自动化协议(SCAP)标准来定义安全策略。

SCAP 是基于 XML 的多个规格的框架，如可扩展检查列表配置描述格式(XCCDF)和开放漏洞和评估语言(OVAL)中描述的漏洞。这些规格被封装为 *数据流文件*。

XCCDF 中的清单项目（也称为 *规则*）表达了系统项目所需的配置。例如，规则可以指定没有人可以使用 root 用户帐户通过 SSH 登录主机。规则可以分组到一个或多个 XCCDF 配置集中，允许多个配置集共享规则。

OpenSCAP 扫描程序工具针对规则评估主机上的系统项目，并在资产报告格式(ARF)中生成报告，然后返回到 Satellite 来监控和分析。

表 9.1. OpenSCAP 扫描程序支持的 SCAP Framework 1.3 中的规格

标题	描述	版本
SCAP	安全内容自动化协议	1.3
XCCDF	可扩展配置检查列表描述格式	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	2.0
CVSS	通用漏洞评分系统	2.0

其他资源

- 有关 SCAP 的更多信息，请参阅 [OpenSCAP 项目](#)。

9.2. SATELLITE 中的 SCAP 内容

SCAP 内容是一个 SCAP 数据流文件，其中包含合规性、配置或安全基准的实施。单个数据流通常包含多个 XCCDF 配置集。XCCDF 配置集定义了一个行业标准或自定义安全标准，您可以评估 Satellite 中主机配置的合规性，如通用目的操作系统(OSPP)、健康保险可移植性和责任法案(HIPAA)和 PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9。您可以使用 *定制文件* 根据要求调整现有的 XCCDF 配置集。

在 Satellite 中，您可以使用 SCAP 内容中的 XCCDF 配置集，最终是定制文件来定义 *合规策略*。Satellite 包括 [OpenSCAP 项目](#) 提供的 SCAP 安全指南中的默认 SCAP 内容。

有关如何下载、部署、修改和创建自己的内容的更多信息，请参阅：

- [Red Hat Enterprise Linux 9 安全强化](#)
- [Red Hat Enterprise Linux 8 安全强化](#)
- [Red Hat Enterprise Linux 7 安全指南](#)
- [Red Hat Enterprise Linux 6 安全指南](#)

9.2.1. 支持的 SCAP 版本

Satellite 支持 SCAP 版本 1.2 和 1.3 的内容。

9.3. 合规策略部署选项

您可以使用以下方法之一部署合规策略：

Ansible 部署

您可以使用 Ansible 角色配置主机以进行合规性扫描。

Puppet 部署

您可以使用 Puppet 类和 Puppet 代理配置主机以进行合规性扫描。

手动部署

您可以手动为合规性扫描配置主机。

9.4. 配置合规策略部署方法

使用以下步骤为您选择的方法配置 Satellite 来部署合规策略。在稍后 [创建合规策略](#) 时，您将选择这些方法之一。

Ansible 部署的步骤

1. 导入 `foreman.foreman_scap_client` Ansible 角色。
如需更多信息，请参阅在 [Red Hat Satellite 中使用 Ansible 集成管理配置](#)
2. 将创建的策略和 `foreman.foreman_scap_client` Ansible 角色分配到主机或主机组。
3. 若要触发部署，请手动对主机或主机组运行 Ansible 角色，或者使用远程执行进行常规策略更新来设置周期性作业。
如需更多信息，请参阅 [管理主机中的配置和设置远程作业](#)。

Puppet 部署的步骤

1. 确保 Puppet 已启用。

2. 确保主机上安装了 Puppet 代理。
3. 导入包含 `foreman_scap_client` Puppet 模块的 Puppet 环境。
如需更多信息，请参阅在 [Red Hat Satellite 中使用 Puppet 集成管理配置](#)
4. 将创建的策略和 `foreman_scap_client` Puppet 类分配给主机或主机组。
Puppet 会触发下一次常规运行的部署，也可以手动运行 Puppet。Puppet 默认每 30 分钟运行一次。

手动部署的步骤

- 对于手动部署方法，不需要额外的 Satellite 配置。
有关手动部署的详情，请参考 [红帽知识库 中的使用 Manual Deployment 选项设置 OpenSCAP 策略](#)。

9.5. 列出可用的 SCAP 内容

使用这个流程查看已在 Satellite 中载入的 SCAP 内容。要使用 CLI 而不是 Satellite Web UI，请参阅 [CLI 过程](#)。

前提条件

- 您的用户帐户具有 `view_scap_contents` 权限。

流程

- 在 Satellite Web UI 中，进入到 `Hosts > Compliance - SCAP contents`。

CLI 过程

- 在 Satellite 服务器上运行以下 Hammer 命令：

```
# hammer scap-content list \
--location "My_Location" \
--organization "My_Organization"
```

9.6. 配置 SCAP 内容

您可以上传 SCAP 数据流和定制文件来定义合规策略。

9.6.1. 加载默认 SCAP 内容

通过在 Satellite 服务器上载入默认 SCAP 内容，您可以确保加载 SCAP 安全指南(SSG)中的数据流，并分配给所有机构和位置。

SSG 由 Satellite 服务器的操作系统提供，并安装在 `/usr/share/xml/scap/ssg/content/` 中。请注意，可用的数据流取决于 Satellite 运行的操作系统版本。您只能使用此 SCAP 内容扫描与 Satellite 服务器具有相同次 RHEL 版本的主机。如需更多信息，请参阅 [第 9.6.2 节“为 RHEL 获取支持的 SCAP 内容”](#)。

先决条件

- 您的用户帐户分配了 `create_scap_contents` 权限的角色。

流程

- 在 Satellite 服务器上使用以下 Hammer 命令：

```
# hammer scap-content bulk-upload --type default
```

9.6.2. 为 RHEL 获取支持的 SCAP 内容

您可以在红帽客户门户网站上获取 Red Hat Enterprise Linux 的最新 SCAP 安全指南(SSG)。您必须获取为主机的次要 RHEL 版本指定的 SSG 版本。

流程

1. 在软件包浏览器中访问 [SCAP 安全指南](#)。
2. 在 Version 菜单中，为您的主机运行的 RHEL 的次版本选择最新的 SSG 版本。例如，对于 RHEL 8.6，请选择名为 `lf el8_6` 的版本。
3. 下载软件包 RPM。
4. 从 RPM 中提取 data-stream 文件(`*-ds.xml`)。例如：

```
$ rpm2cpio scap-security-guide-0.1.69-3.el8_6.noarch.rpm |
| cpio -iv --to-stdout ./usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml |
> ssg-rhel-8.6-ds.xml
```

5. 将数据流上传到 Satellite。如需更多信息，请参阅 [第 9.6.3 节“上传额外的 SCAP 内容”](#)。

其他资源

- [红帽知识库 中的 RHEL 中支持的 SCAP 安全指南版本](#)
- [Red Hat Enterprise Linux 9 安全强化中的 RHEL 9 支持的 SCAP 安全指南配置文件](#)
- [Red Hat Enterprise Linux 8 安全强化中的 RHEL 8 支持的 SCAP 安全指南配置文件](#)
- [Red Hat Enterprise Linux 7 安全指南中 RHEL 7 支持的 SCAP 安全指南配置文件](#)

9.6.3. 上传额外的 SCAP 内容

您可以将其他 SCAP 内容上传到 Satellite 服务器，可以是自己创建的内容，或者在其他位置获取。请注意，红帽只提供对从红帽获取的 SCAP 内容的支持。要使用 CLI 而不是 Satellite Web UI，请参阅 [CLI 过程](#)。

前提条件

- 您的用户帐户具有 `create_scap_contents` 权限。
- 您已获取了 SCAP 数据流文件。

流程

1. 在 Satellite Web UI 中，进入到 Hosts > Compliance > SCAP contents。

2. 单击 **Upload New SCAP Content**。
3. 在 **Title** 文本框中输入标题，如 **My SCAP Content**。
4. 在 **Scap File** 中，单击 **Choose file**，导航到包含 SCAP data-stream 文件的位置，然后单击 **Open**。
5. 在 **位置** 选项卡上，选择位置。
6. 在 **组织** 选项卡上，选择组织。
7. 点 **Submit**。

如果成功加载 SCAP 内容文件，则会显示类似于 **Successfully created My SCAP Content** 的消息。

CLI 过程

1. 将 SCAP data-stream 文件放在 Satellite 服务器上的目录中，如 `/usr/share/xml/scap/my_content/`。
2. 在 Satellite 服务器上运行以下 Hammer 命令：

```
# hammer scap-content bulk-upload --type directory \
--directory /usr/share/xml/scap/my_content/ \
--location "My_Location" \
--organization "My_Organization"
```

验证

- 列出可用的 SCAP 内容。SCAP 内容列表包含新标题。

9.6.4. 定制 XCCDF 配置集

您可以使用定制文件自定义现有的 XCCDF 配置集，而无需编辑原始 SCAP 内容。单个定制文件可以包含多个 XCCDF 配置集的自定义。

您可以使用 [SCAP Workbench](#) 工具创建定制文件。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](#)。

然后，您可以将定制文件分配给合规策略，以在策略中自定义 XCCDF 配置集。

9.6.5. 上传定制文件

上传定制文件后，您可以在自定义策略中应用它来自定义 XCCDF 配置集。

前提条件

- 您的用户帐户具有 `create_tailoring_files` 权限。

流程

1. 在卫星 Web UI 中，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**，导航到包含定制文件的位置，然后选择 **Open**。
4. 单击 **Submit** 以上传所选的定制文件。

9.7. 管理合规策略

合规策略是一个调度的审计，用于检查指定的主机是否符合 SCAP 内容中的特定 XCCDF 配置集。

您可以指定 Satellite 服务器上扫描的调度，并在主机上执行扫描。扫描完成后，会生成 ARF 格式的报告并上传到 Satellite 服务器。合规策略不对扫描的主机进行任何更改。

合规策略定义 SCAP 客户端配置和 cron 计划。然后，策略会与分配策略的主机上的 SCAP 客户端一起部署。

9.7.1. 创建合规策略

通过创建合规策略，您可以定义和规划安全合规要求，并确保您的主机保持符合您的安全策略。

先决条件

- 您已为所选 [合规策略部署方法](#) 配置了 Satellite。
- 您已在 Satellite 中可用 SCAP 内容，最终定制文件。
 - 要验证可用的 SCAP 内容，请参阅 [第 9.5 节“列出可用的 SCAP 内容”](#)。
 - 要上传 SCAP 内容和定制文件，请参阅 [第 9.6 节“配置 SCAP 内容”](#)。
- 您的用户帐户具有 `view_policies` 和 `create_policies` 权限。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > Compliance - Policies**。
2. 单击 **New Policy** 或 **New Compliance Policy**。
3. 选择部署方法：**Ansible**、**Puppet** 或 **Manual**。然后单击“下一步”。
4. 输入此策略的名称、描述（可选），然后单击下一步。
5. 选择要应用的 SCAP Content 和 XCCDF Profile，然后单击 **Next**。
请注意，Satellite 不会检测所选 XCCDF 配置集是否包含任何规则。一个空的 XCCDF 配置集（如 **Default XCCDF Profile**）将返回空的报告。
6. 可选：要自定义 XCCDF 配置集，请选择 **Tailoring File** 和 **XCCDF Profile in Tailoring File**，然后点 **Next**。
7. 指定应用策略时的调度时间。从 **Period** 列表中选择 **Weekly**、**Monthly** 或 **Custom**。**Custom** 选项允许在策略调度中更大的灵活性。
 - 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**，还在 **Day of month** 字段中指定了日期。
 - 如果您选择 **Custom**，在 **Cron line** 字段中输入有效的 Cron 表达式。

8. 选择要应用策略的位置，然后单击 Next。
9. 选择要应用该策略的组织，然后单击下一步。
10. 可选：选择要为其分配策略的主机组。
11. 点 Submit。

9.7.2. 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。当您计划策略时，这非常有用。

前提条件

- 您的用户帐户具有 `view_policies` 权限。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Compliance - Policies。
2. 在所需策略的 Actions 列中，点 Show Guide 或从列表中选择它。

9.7.3. 编辑合规策略

在卫星 Web UI 中，您可以编辑合规性策略。

Puppet 代理在下次运行时将编辑的策略应用到主机。默认情况下，每 30 分钟发生一次。如果使用 Ansible，您必须手动运行 Ansible 角色，或者配置了在主机上运行 Ansible 角色的周期性远程执行作业。

前提条件

- 您的用户帐户具有 `view_policies` 和 `edit_policies` 权限。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Compliance - Policies。
2. 点所需策略的名称。
3. 编辑必要的属性。
4. 点 Submit。

9.7.4. 删除合规策略

在卫星 Web UI 中，您可以删除现有合规策略。

前提条件

- 您的用户帐户具有 `view_policies` 和 `destroy_policies` 权限。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Compliance - Policies。

2. 在所需策略的 Actions 列中，从列表中选择 Delete。
3. 在确认消息中点 OK。

9.8. 部署合规策略

若要部署合规策略，您必须安装 SCAP 客户端，更新 cron 调度文件，并将策略中选择的 SCAP 内容上传到主机上。

9.8.1. 使用 Ansible 在主机组中部署策略

使用 Ansible 在主机组中部署合规策略后，Ansible 角色将安装 SCAP 客户端并根据所选的合规策略在主机上配置 OpenSCAP 扫描。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 [Capsule 服务器](#) 中的 [在 Capsule 服务器上启用 OpenSCAP](#)。
- 您已启用并将操作系统存储库同步到 Satellite，并在主机上启用它们：
 - Red Hat Enterprise Linux 9 for x86_64 - BaseOS 和 Appstream (RPMs)- `rhel-9-for-x86_64-baseos-rpms` 和 `rhel-9-for-x86_64-appstream-rpms`
 - Red Hat Enterprise Linux 8 for x86_64 - BaseOS 和 Appstream (RPMs)- `rhel-8-for-x86_64-baseos-rpms` 和 `rhel-8-for-x86_64-appstream-rpms`
 - Red Hat Enterprise Linux 7 Server 和 Extras (RPMs)- `rhel-7-server-rpms` 和 `rhel-7-server-extras-rpms`
- 您已启用并将 Satellite 客户端 6 存储库同步到 Satellite，并在主机上启用它。
- 您已使用 Ansible 部署选项 [创建了合规策略](#)，并分配了主机组。

流程

1. 在 Satellite Web UI 中，进入到 Configure > Host Groups。
2. 点您要为 OpenSCAP 报告配置的主机组。
3. 在 OpenSCAP Capsule 列表中，选择启用的 OpenSCAP 的胶囊。
4. 在 Ansible Roles 选项卡上，分配 `foreman.foreman_scap_client` Ansible 角色。
5. 可选：在 Parameters 选项卡中，配置角色的任何 Ansible 变量。
6. 点 Submit 保存您的更改。
7. 在所需主机组的行中，导航到 Actions 列，再选择 Run all Ansible roles。

9.8.2. 使用 Ansible 在主机上部署策略

使用 Ansible 在主机上部署合规策略后，Ansible 角色将安装 SCAP 客户端并根据所选的合规策略在主机上配置 OpenSCAP 扫描。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 [Capsule 服务器](#) 中的 [在 Capsule 服务器上启用 OpenSCAP](#)。
- 您已启用并将操作系统存储库同步到 Satellite，并在主机上启用它们：
 - Red Hat Enterprise Linux 9 for x86_64 - BaseOS 和 Appstream (RPMs)- [rhel-9-for-x86_64-baseos-rpms](#) 和 [rhel-9-for-x86_64-appstream-rpms](#)
 - Red Hat Enterprise Linux 8 for x86_64 - BaseOS 和 Appstream (RPMs)- [rhel-8-for-x86_64-baseos-rpms](#) 和 [rhel-8-for-x86_64-appstream-rpms](#)
 - Red Hat Enterprise Linux 7 Server 和 Extras (RPMs)- [rhel-7-server-rpms](#) 和 [rhel-7-server-extras-rpms](#)
- 您已启用并将 Satellite 客户端 6 存储库同步到 Satellite，并在主机上启用它。
- 您已使用 Ansible 部署选项 [创建了合规策略](#)。

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 OpenSCAP Capsule 列表中，选择启用的 OpenSCAP 的胶囊。
3. 在 Ansible Roles 选项卡上，添加 `foreman.foreman_scap_client` Ansible 角色。
4. 可选：在 Parameters 选项卡中，配置角色的任何 Ansible 变量。
5. 点 Submit 保存您的更改。
6. 单击 Hosts breadcrumbs 链接，以返回主机索引页面。
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 Assign Compliance Policy 窗口中，为下一个批量操作选择 Remember hosts。
11. 从可用策略列表中选择所需的策略，然后单击 Submit。
12. 点 Select Action。
13. 从列表中选择 Run all Ansible roles。

9.8.3. 使用 Puppet 在主机组中部署策略

使用 Puppet 在主机组中部署合规策略后，Puppet 代理将安装 SCAP 客户端，并根据所选的合规性策略在下一个 Puppet 上的主机上配置 OpenSCAP 扫描。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 [Capsule 服务器中的在 Capsule 服务器上启用 OpenSCAP](#)。
- 您已启用并将操作系统存储库同步到 Satellite，并在主机上启用它们：
 - Red Hat Enterprise Linux 9 for x86_64 - BaseOS 和 Appstream (RPMs)- `rhel-9-for-x86_64-baseos-rpms` 和 `rhel-9-for-x86_64-appstream-rpms`
 - Red Hat Enterprise Linux 8 for x86_64 - BaseOS 和 Appstream (RPMs)- `rhel-8-for-x86_64-baseos-rpms` 和 `rhel-8-for-x86_64-appstream-rpms`
 - Red Hat Enterprise Linux 7 Server 和 Extras (RPMs)- `rhel-7-server-rpms` 和 `rhel-7-server-extras-rpms`
- 您已启用并将 Satellite 客户端 6 存储库同步到 Satellite，并在主机上启用它。
- 您已使用 Puppet 部署选项 [创建了合规策略](#)，并分配了主机组。

流程

1. 在 Satellite Web UI 中，进入到 Configure > Host Groups。
2. 点您要为 OpenSCAP 报告配置的主机组。
3. 在 Environment 列表中，选择包含 `foreman_scap_client*` Puppet 类的 Puppet 环境。
4. 在 OpenSCAP Capsule 列表中，选择启用了 OpenSCAP 的 Capsule。
5. 在 Puppet ENC 选项卡中，添加 `foreman_scap_client` Puppet 类。
6. 可选：配置任何 Puppet 类参数。
7. 点 Submit 保存您的更改。

9.8.4. 使用 Puppet 在主机上部署策略

使用 Puppet 在主机上部署合规策略后，Puppet 代理将安装 SCAP 客户端，并根据所选的合规策略在下次 Puppet 的主机上配置 OpenSCAP 扫描。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 [Capsule 服务器中的在 Capsule 服务器上启用 OpenSCAP](#)。
- 您已启用并将操作系统存储库同步到 Satellite，并在主机上启用它们：
 - Red Hat Enterprise Linux 9 for x86_64 - BaseOS 和 Appstream (RPMs)- `rhel-9-for-x86_64-baseos-rpms` 和 `rhel-9-for-x86_64-appstream-rpms`
 - Red Hat Enterprise Linux 8 for x86_64 - BaseOS 和 Appstream (RPMs)- `rhel-8-for-x86_64-baseos-rpms` 和 `rhel-8-for-x86_64-appstream-rpms`
 - Red Hat Enterprise Linux 7 Server 和 Extras (RPMs)- `rhel-7-server-rpms` 和 `rhel-7-server-extras-rpms`
- 您已启用并将 Satellite 客户端 6 存储库同步到 Satellite，并在主机上启用它。

- 您已使用 Puppet 部署选项 [创建了合规策略](#)。

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. 从 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. 在 Puppet ENC 选项卡中，添加 foreman_scap_client Puppet 类。
5. 可选：配置任何 Puppet 类参数。
6. 单击 Hosts breadcrumbs 链接，以返回主机索引页面。
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 Assign Compliance Policy 窗口中，为下一个批量操作选择 Remember hosts。
11. 从可用策略列表中选择所需的策略，然后单击 Submit。

9.9. 对需求运行安全合规扫描

主机由分配给主机的合规策略中定义的 CRON 调度定期执行 OpenSCAP 扫描。但是，您也可以随时手动针对所有配置的合规策略在主机上运行扫描。

先决条件

- 您的用户帐户具有 view_hosts、create_job_invocations 和 view_job_invocations 权限。
- 您已创建了安全策略并将其部署到主机上。
 - 有关管理策略的更多信息，请参阅 [第 9.7 节“管理合规策略”](#)。
 - 有关部署策略的更多信息，请参阅 [第 9.8 节“部署合规策略”](#)。

流程

1. 导航到 Hosts > All Hosts。
2. 点所需主机的主机名。
3. 在主机详情页面上，展开 Schedule a job 下拉菜单。
4. 选择 Run OpenSCAP scan。

验证

1. 在主机详情概述中找到 Recent 作业卡。

2. 选择 **Running** 选项卡。除非作业已完成，表显示所有 OpenSCAP 策略的 Run scan 作业。
3. 在 **Recent jobs** 卡中，选择 **Finished** 选项卡。
4. 如果作业成功完成，您应该在作业所在行中看到 **succeeded** 状态。
5. 可选：点击作业名称来查看调用详情。

9.10. 监控合规性

借助 Satellite，您可以集中进行合规监控和管理。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。通过监控 SCAP 合规性，您可以验证策略合规性并检测合规性中的更改。

9.10.1. 搜索合规性报告

使用 **Compliance Reports** 搜索字段过滤对任何主机子集的可用报告列表。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > Reports**。
2. 可选：要查看可用搜索参数列表，请点击空 **Search** 字段。
3. 在 **Search** 字段中输入搜索查询，然后单击 **Search**。搜索查询不区分大小写。

搜索查询示例

查找超过五个规则失败的所有合规性报告

```
failed > 5
```

查找 2023 年 1 月 1 日之后创建的所有合规性报告，以用于包含 **prod-** 的主机名的主机。

```
host ~ prod- AND date > "Jan 1, 2023"
```

从一小时前查找 **rhel7_audit** 合规策略生成的所有报告

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

查找通过 XCCDF 规则的报告

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

查找没有 XCCDF 规则的报告

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

查找与 XCCDF 规则不同的结果或不通过的报告

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

其它信息

- 您可以针对以下逻辑运算符创建复杂的查询：**and**、**not** 和 **has**。有关逻辑运算符的更多信息，请参阅管理 Red Hat Satellite 中的 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，请参阅管理 Red Hat Satellite 中的 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。如需更多信息，请参阅管理 Red Hat Satellite 中的 创建书签。

9.10.2. 合规电子邮件通知

Satellite 服务器向订阅合规策略摘要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更多信息，请参阅第 8.2 节“配置电子邮件通知首选项”。

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。

9.10.3. 查看合规策略统计

您可以查看合规策略仪表盘，以验证特定策略的合规性报告。合规策略控制面板提供主机合规性的统计信息，以及查看该策略范围内每个主机的报告详细信息的能力。

在查看合规报告时，请考虑优先选择以下主机：

- 被评估为 **Failed** 的主机
- 标记为 **Never** 审计的主机，因为它们的状态为 **unknown**

前提条件

- 您的用户帐户具有 **view_policies** 权限。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Policies。
2. 在所需策略所在的行中，导航到 Actions 列，再单击 Dashboard。

9.10.4. 检查每个规则合规结果的主机

您可以检查简化的报告，并使用策略规则列出具有特定合规性结果的主机，如特定规则失败。

前提条件

- 您的用户帐户具有 **view_arf_reports** 和 **view_hosts** 权限。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Reports。

2. 在 **Reported At** 列中，导航到所需主机和合规策略的报告，然后单击时间链接。
3. Satellite 使用扫描结果显示简化的策略规则列表。
4. 可选：通过检查结果过滤规则。从 **Show log messages** 下拉列表中，选择以下过滤器之一：
 - 失败和其他 - 查看扫描期间或未检查的规则，
 - 仅失败 - 仅查看失败的规则。
5. 可选：检查规则的详情。在 **Message** 列中，单击规则名称旁边的图标。
6. 在必要规则的行中，导航到 **Actions** 列，再单击 **Hosts failing this rule**。

9.10.5. 检查主机的合规性故障

您可以检查完整的合规性报告，确定主机对规则是否合规的原因，在某些情况下，请参阅如何修复不合规的情况。



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。补救可能会导致系统无法正常工作。

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

前提条件

- 您的用户帐户具有 **view_arf_reports** 和 **view_hosts** 权限。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > Reports** 以列出所有合规性报告。
2. 在所需主机的行中，导航到 **Actions** 列，再单击 **Full Report** 以查看评估报告的完整详情。
3. 导航到 **Evaluation Characteristics** 区域，以查看有关针对特定配置文件评估主机的基本详情。
4. 导航到 **Compliance** 和 **Scoring** 区域，以检查评估统计信息和主机合规性分数。
5. 导航到 **Rule Overview** 以检查规则。
6. 可选：取消选择您要隐藏的检查状态，如 **通过**、**不可应用** 或 **固定**。

7. 可选：在组规则下拉菜单中，选择规则分组条件，如严重性。
8. 可选：在搜索字段中输入搜索字符串，以根据标题过滤规则。在输入时，搜索是区分大小写的，并动态应用。
9. 点规则的标题检查进一步的结果详情：
 - 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。

9.10.6. 删除合规性报告

您可以删除 Satellite 的合规性报告。

前提条件

- 您的用户帐户具有 `view_arf_reports` 和 `destroy_arf_reports` 权限。

流程

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. 点击确定。

9.10.7. 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 API 指南中的 [删除 OpenSCAP 报告](#) 中的脚本。

前提条件

- 您的用户帐户具有 `view_arf_reports` 和 `destroy_arf_reports` 权限。

流程

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。

第 10 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。

+



注意

如果您创建 Satellite 服务器的新实例，请在恢复备份后停用旧实例。克隆的实例不应在生产环境中并行运行。

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 10.5 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 8 配置基本系统设置中的[修复和恢复系统](#)。



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 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
```

10.1. 估算备份的大小

完整备份创建 PostgreSQL 和 Pulp 数据库文件，以及 Satellite 配置文件的未压缩存档。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/lib/pgsql/data /var/lib/pulp
100G /var/lib/pgsql/data
100G /var/lib/pulp

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

2. 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 10.1. 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	<code>/var/lib/pgsql/data</code>	80–85%	100 GB → 20 GB
Pulp RPM 文件	<code>/var/lib/pulp</code>	(未压缩)	100 GB
配置文件	<code>/var/lib/qpidd</code> <code>/var/lib/tftpboot</code> <code>/etc</code> <code>/root/ssl-build</code> <code>/var/www/html/pub</code> <code>/opt/puppetlabs</code>	85%	942 MB → 141 MB

在本例中，压缩备份数据总占用 120 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 201 GB 加上 120 GB 用于未压缩备份数据 321 GB。具有 64 GB 的额外空间，必须为备份位置分配 385 GB。

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

Red Hat Satellite 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**
有关这些方法的更多信息，您可以查看每种备份方法的使用声明。

离线备份

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

在线备份

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

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 PostgreSQL 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 10.1 节“估算备份的大小”](#)。



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。

流程

- 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
```

10.3. 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。对于生产环境用例，请不要从不包含 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 10.1 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
```

10.4. 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 10.1 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
```

10.5. 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 --assumeeyes $DESTINATION
else
    LAST=$(ls -td -- $DESTINATION/* | head -n 1)
    satellite-maintain backup offline --assumeeyes --incremental "$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 `--assumeeyes` 选项则用于跳过确认提示。

10.6. 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 10.7 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 10.1 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
```

10.7. 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

- 系统将 LVM 用于您快照的目录：`/var/lib/pulp/` 和 `/var/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 backup snapshot` 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。

10.8. 在执行备份时列出和跳过步骤

使用 `satellite-maintain backup` 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。

流程

- 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 11 章 从备份中恢复 SATELLITE 服务器或胶囊服务器

您可以从您创建的备份数据恢复 Satellite 服务器或胶囊服务器，作为 [第 10 章 备份 Satellite 服务器和胶囊服务器](#) 的一部分。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。

11.1. 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到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，请按照在 [连接的网络环境中安装卫星服务器](#) 中的步骤。
 - 要从断开连接的网络安装 Satellite 服务器，请按照在 [断开连接的网络环境中安装卫星服务器](#) 中的步骤。
 - 要安装胶囊服务器，请遵循 [安装胶囊服务器](#) 中的步骤。
2. 将备份数据复制到 Satellite 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`。

11.2. 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，请按时间顺序为您要恢复的分支选择完整备份以及每个增量备份。

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 11.1 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 Satellite 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 /var/backup_directory/FIRST_INCREMENTAL
# satellite-maintain restore /var/backup_directory/SECOND_INCREMENTAL
```

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`。

11.3. 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，直到您可以在卫星 Web UI 中确认，该胶囊服务器已连接到卫星服务器。然后使用第 11.3.1 节“同步外部胶囊”过程从 Satellite 同步。

11.3.1. 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，请在卫星 Web UI 中选择相关组织和位置，或者选择 Any Organization 和 Any Location。
2. 在 Satellite Web UI 中，导航到 Infrastructure > Capsules，再单击要同步的胶囊名称。
3. 在 Overview 选项卡中，选择 Synchronize。

第 12 章 重命名 SATELLITE SERVER 或 CAPSULE SERVER

要重命名 Satellite 服务器或胶囊服务器，请使用 `satellite-change-hostname` 脚本。



重要

在更改 Satellite 服务器或 Capsule 服务器的域名时，使用 `satellite-change-hostname` 更新主机名，以避免网络问题。

12.1. 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。此流程可确保除了重命名 Satellite 服务器外，您还可以更新所有引用以指向新的主机名。



警告

重命名您的 Satellite 服务器主机会关闭该主机上的所有 Satellite 服务。重命名完成后服务会重启。

先决条件

- 在更改其主机名前备份您的 Satellite 服务器。如果您无法成功重命名，请从备份中恢复。更多信息请参阅 [第 10 章 备份 Satellite 服务器和胶囊服务器](#)。
- 在 Satellite 服务器上运行主机名和 `主机名 -f` 命令。如果这两个命令没有返回 Satellite 服务器的 FQDN，则 `satellite-change-hostname` 脚本将无法完成。如果 `hostname` 命令返回 Satellite 服务器的短名称而不是 FQDN，请使用 `hostnamectl set-hostname My_Old_FQDN`，然后再使用 `satellite-change-hostname` 脚本正确设置旧的 FQDN。
- 如果 Satellite 服务器安装了自定义 SSL 证书，请为主机的新 FQDN 获取新证书。有关更多信息，请参阅 [在连接的网络环境中安装卫星服务器时使用自定义 SSL 证书配置卫星服务器](#)。

流程

1. 在命令行中，运行 `satellite-change-hostname` 脚本，并提供新的主机名。选择以下任一方法：

- 如果您的 Satellite 服务器安装了默认自签名 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 \  
--ssl-certificate /path/to/certificate
```

```
--custom-cert "/root/ownca/test.com/test.com.crt" \  
--custom-key "/root/ownca/test.com/test.com.key"
```

2. 如果您已经为新的 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 [在连接的网络环境中安装 Satellite 服务器中的向 Satellite 服务器部署自定义 SSL 证书](#)。
3. 重新注册所有 Satellite 主机。如需更多信息，请参阅 [管理主机](#) 中的 [注册主机](#)。
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 https://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 My_capsule_ID
```

7. 如果使用 virt-who 代理，请使用新的主机名更新 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](#)。
8. 如果使用外部身份验证，请在运行 `satellite-change-hostname` 脚本后重新配置 Satellite 服务器以进行外部身份验证。如需更多信息，请参阅 [在连接的网络环境中安装 Satellite 服务器中的配置外部身份验证](#)。

12.2. 重命名胶囊服务器

Capsule 服务器的主机名由 Satellite 服务器组件和注册的所有主机引用。此流程可确保除了重命名胶囊服务器外，您也更新对新主机名的所有引用。



警告

重命名您的胶囊服务器主机会关闭该主机上的所有 Satellite 服务。重命名完成后服务会重启。

先决条件

- 在重命名前备份您的 Capsule 服务器。如果您无法成功重命名，请从备份中恢复。更多信息请参阅 [第 10 章 备份 Satellite 服务器和胶囊服务器](#)。
- 在 Capsule 服务器上运行主机名和 `主机名 -f` 命令。如果这两个命令没有返回 Capsule 服务器的 FQDN，则 `satellite-change-hostname` 脚本将无法完成。

如果 `hostname` 命令返回 Capsule 服务器的短名称, 而不是 FQDN, 请在尝试使用 `satellite-change-hostname` 脚本前, 使用 `hostnamectl set-hostname My_Old_FQDN` 来正确设置旧的 FQDN。

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。有关更多信息, 请参阅安装 Capsule 服务器中的 [使用自定义 SSL 证书配置 Capsule 服务器](#)。
2. 在受管主机上, 将证书存档文件复制到胶囊服务器。例如, 将存档文件复制到 `root` 用户的主目录:

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

3. 在 Capsule 服务器上, 运行 `satellite-change-hostname` 脚本, 并提供主机的新名称、Satellite 凭据和证书存档文件名。

```
# satellite-change-hostname new-capsule.example.com --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. 如果您为 Capsule 服务器创建了自定义证书, 请输入在上一步中返回的 `satellite-installer` 命令, 在 Capsule 服务器上部署证书。如需更多信息, 请参阅 [安装 Capsule 服务器中的向 Capsule 服务器部署自定义 SSL 证书](#)。

- 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](#)。

```
# dnf remove katello-ca-consumer*  
  
# dnf install http://new-capsule.example.com/pub/katello-ca-consumer-latest.noarch.rpm  
  
# subscription-manager register --org="My_Organization" \  
--environment="Library" \  
--force
```

```
--force
```

```
# subscription-manager refresh
```

6.

在 Satellite Web UI 中更新 Capsule 主机名。

a.

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

b.

在列表中找到 Capsule Server，然后单击 Edit。

c.

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。

d.

在 DNS 服务器上，为您的胶囊服务器的新主机名添加记录，并删除之前主机名的记录。

第 13 章 维护 SATELLITE 服务器

本章提供了有关如何维护卫星服务器的信息，包括如何使用审计记录、清理未使用的任务以及如何从完整磁盘中恢复 Pulp。

13.1. 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
```

13.2. 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 `anonymizes 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
```

13.3. 删除 REPORT RECORDS

在 Satellite 中会自动创建报告记录。您可以使用 `foreman-rake reports:expire` 命令随时删除报告。您还可以使用 `cron` 作业以设定的时间间隔来调度报告记录删除。

默认情况下，使用 `foreman-rake reports:expire` 命令删除超过 90 天的报告记录。您可以通过添加

days 选项并添加天数来指定保留报告记录的天数。

例如，如果您想要删除超过七天的报告记录，请输入以下命令：

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

13.4. 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

您可以使用以下选项配置清理未使用的任务功能：

- 要配置 Satellite 运行 cron 作业的时间，请将 `--foreman-plugin-tasks-cron-line` 参数设置为您想要的时间(cron 格式)。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 * * *"
```

- 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。

- 要禁用 Satellite 上的常规任务清理，请输入以下命令：

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

- 要在 Satellite 上重新启用常规任务清理，请输入以下命令：


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

13.5. 删除任务记录

在卫星中自动创建任务记录。您可以使用 `foreman-rake foreman_tasks:cleanup` 命令删除所有任务。您还可以使用 `cron` 作业以设定的时间间隔来调度任务记录删除。

例如，如果要从成功存储库同步中删除任务记录，请输入以下命令：

```
# foreman-rake foreman_tasks:cleanup TASK_SEARCH='label = Actions::Katello::Repository::Sync'
STATES='stopped'
```

13.6. 按 ID 删除任务

您可以按 ID 删除任务，例如，如果您错误地提交了机密数据。

流程

1. 使用 SSH 连接到您的 Satellite 服务器：

```
# ssh root@satellite.example.com
```

2. 可选：查看任务：

```
# hammer task info --id My_Task_ID
```

3. 删除任务：

```
# foreman-rake foreman_tasks:cleanup TASK_SEARCH="id=My_Task_ID"
```

4. 可选：确保任务已从 Satellite Server 中删除：

```
# hammer task info --id My_Task_ID
```

请注意，因为任务被删除，这个命令会返回非零退出代码。

13.7. 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。

流程

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 8 配置和管理逻辑卷 中的 [增大逻辑卷和文件系统](#)。

**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** 服务：

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

2.

在 LV 上增加文件系统。

3.

启动 **Satellite** 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。

13.8. 在卫星服务器或胶囊服务器基本操作系统上管理软件包

要在 **Satellite Server** 或 **Capsule Server** 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** 服务器或 **Capsule** 服务器相关的软件包，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 Server** 或 **Capsule Server** 上安装软件包，请输入以下命令：

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

•

要在 **Satellite Server** 或 **Capsule Server** 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 服务器** 或 **Capsule Server** 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在卫星服务器或胶囊服务器中打包不一致。有关在 **Satellite 服务器** 中更新软件包的更多信息，请参阅 [更新 Satellite 服务器](#)。

为 **Satellite Server** 或 **Capsule Server 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 Server** 或 **Capsule Server**，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
```

13.9. 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 --all'
```

3.

vacuum 完成后启动其他服务：

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

第 14 章 续订自定义 SSL 证书

本章介绍了如何在 **Satellite 服务器** 和 **Capsule 服务器** 上更新自定义 **SSL 证书**。

14.1. 在 **SATELLITE 服务器** 上续订自定义 **SSL 证书**

使用这个流程为 **Satellite 服务器** 更新自定义 **SSL 证书**。

前提条件

- 您必须创建新的证书签名请求(CSR)，并将其发送到证书颁发机构以签署证书。创建新 CSR 前，请参阅 [配置 Satellite 服务器](#) 指南，因为服务器证书必须具有 X.509 v3 密钥使用 和扩展密钥用法 扩展。在返回中，您将收到 **Satellite 服务器证书** 和 **CA 捆绑包**。

流程

- 在 **Satellite 服务器** 上部署续订的自定义证书前，请验证自定义 **SSL 输入文件**。请注意，对于 `katello-certs-check` 命令正常工作，证书中的通用名称(CN)必须与 **Satellite 服务器** 的 **FQDN 匹配**：

```
# katello-certs-check -t satellite \
-b /root/satellite_cert/ca_cert_bundle.pem \
-c /root/satellite_cert/satellite_cert.pem \
-k /root/satellite_cert/satellite_cert_key.pem
```

如果命令成功，它会返回以下 `satellite-installer` 命令。您可以使用此命令将更新的 **CA 证书** 部署到 **Satellite 服务器**：

```
# satellite-installer --scenario satellite \
--certs-server-cert "/root/satellite_cert/satellite_cert.pem" \
--certs-server-key "/root/satellite_cert/satellite_key.pem" \
--certs-server-ca-cert "/root/satellite_cert/ca_cert_bundle.pem" \
--certs-update-server \
--certs-update-server-ca
```

重要

部署证书后不要删除证书文件。升级 **Satellite 服务器** 时需要它们。



注意

如果因为不同的证书签名请求授权机构生成了新的消费者软件包 `katello-ca-consumer-latest.noarch.rpm`，则必须更新注册到 **Satellite** 服务器的所有客户端。

验证

1. 从本地机器访问 **Satellite Web UI**。例如：<https://satellite.example.com>。
2. 在您的浏览器中，查看证书详情以验证部署的证书。

14.2. 在 CAPSULE 服务器上续订自定义 SSL 证书

使用这个流程为 **Capsule** 服务器更新自定义 **SSL** 证书。`satellite-installer` 命令返回 `Capsule -certs-generate` 命令对于每个胶囊服务器都是唯一的。您不能在多个胶囊服务器上使用相同的命令。

前提条件

- 您必须创建新的证书签名请求，并将其发送到证书颁发机构以签署证书。创建新 **CSR** 前，请参阅 [配置 Satellite 服务器指南](#)，因为 **Satellite** 服务器证书必须具有带有所需值的 **X.509 v3** 密钥使用 和扩展密钥使用扩展。在返回中，您将收到 **Capsule** 服务器证书和 **CA** 捆绑包。

流程

1. 在 **Satellite** 服务器上，验证自定义 **SSL** 证书输入文件：

```
# katello-certs-check -t capsule \
-b /root/capsule_cert/ca_cert_bundle.pem \
-c /root/capsule_cert/capsule_cert.pem \
-k /root/capsule_cert/capsule_cert_key.pem
```

2. 在 **Satellite** 服务器上，为您的 **Capsule** 服务器生成证书存档文件：

```
capsule-certs-generate --foreman-proxy-fqdn "capsule.example.com" \
--certs-tar "/root/My_Certificates/capsule.example.com-certs.tar" \
--server-cert "/root/My_Certificates/capsule_cert.pem" \
--server-key "/root/My_Certificates/capsule_cert_key.pem" \
--server-ca-cert "/root/My_Certificates/ca_cert_bundle.pem" \
--certs-update-server
```

3.

在 **Satellite 服务器**上，将证书归档文件复制到您的 **Capsule 服务器**中：

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

如果需要，您可以将复制的文件移到适用路径中。

4.

保留 **Capsule- certs-generate** 命令返回的 **satellite- installer** 命令的副本，以将证书部署到您的胶囊服务器。

5.

使用 **Capsule- certs-generate** 命令返回的 **satellite-installer** 命令将证书部署到 **Capsule 服务器**上：

```
# satellite-installer --scenario capsule \  
--foreman-proxy-register-in-foreman "true" \  
--foreman-proxy-foreman-base-url "https://satellite.example.com" \  
--certs-tar-file "/root/My_Certificates/capsule.example.com-certs.tar" \  
--certs-update-server
```



重要

部署证书后，不要删除 **Capsule 服务器**上的证书存档文件。升级 **Capsule 服务器**时需要它们。



注意

如果因为不同的证书签名请求授权而生成了新的消费者软件包 **katello-ca-consumer-latest.noarch.rpm**，则必须更新注册到 **Capsule 服务器**的所有客户端。

第 15 章 日志记录和报告问题

本章提供了有关如何在 **Satellite** 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、如何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
```

15.1. 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** 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** 的详细调试信息。

流程

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
```

15.2. 通过调试增加日志记录级别

默认情况下，卫星附带了 **:INFO** 级别日志记录。您可以增加或减少 **Satellite** 上的日志级别。

在所有组件中启用 **debug** 级别的日志记录

```
# hammer admin logging --all --level-debug  
# satellite-maintain service restart
```

为特定组件启用 **debug** 级别日志记录

```
# hammer admin logging --components "Component" --level-debug
```

将 **debug** 级别日志记录恢复为 **INFO**

```
# hammer admin logging --all --level-production
# satellite-maintain service restart
```

列出所有组件和更改的配置文件

```
# hammer admin logging --list
-----|-----|-----
COMPONENT | AUTO-DETECTED BY EXISTENCE OF | DESTINATIONS
-----|-----|-----
dhcpd     | /etc/dhcp/dhcpd.conf           | syslog /var/log/dhcpd-debug.log
postgresql | /var/lib/pgsql/data/postgresql.conf | syslog /var/lib/pgsql/data/pg_log/
proxy     | /etc/foreman-proxy/settings.yml | /var/log/foreman-proxy/proxy.log
qpidd     | /etc/qpidd/qpidd.conf          | syslog
rails     | /etc/foreman/settings.yaml     | /var/log/foreman/production.log
tomcat    | /etc/candlepin/candlepin.conf  | /var/log/candlepin/ /var/log/tomcat/
virt-who  | /etc/sysconfig/virt-who        | syslog
-----|-----|-----
```

15.2.1. 为 Hammer 增加日志记录级别

您可以在 `~/.hammer/log/hammer.log` 中找到 Hammer 的日志。编辑 `/etc/hammer/cli_config.yml` 并设置 `:log_level:`

```
:log_level: 'debug'
```

15.2.2. 在 Capsule 上增加日志记录级别

您可以在 `/var/log/foreman-proxy/proxy.log` 中找到 Capsule 的日志。取消注释 `/etc/foreman-proxy/settings.yml` 中的 `DEBUG` 行：

```
:log_level: DEBUG
```

确保重启后重启 `foreman-proxy` 服务：

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

小心

运行安装程序将会恢复这个更改。

15.2.3. 为 Candlepin 增加日志记录级别

您可以在 `/var/log/candlepin/candlepin.log` 中找到 `Candlepin.log` 的日志。错误也会记录到单独的文件中，以便更轻松地进行调试 `/var/log/candlepin/error.log`。

扩展 `/etc/candlepin/candlepin.conf`：

```
log4j.logger.org.candlepin=DEBUG
```

确保重启后重启 `tomcat` 服务：

```
# systemctl restart tomcat
```

如果 `candlepin` 日志文件过于详细，您可以降低默认的调试级别：

```
log4j.logger.org.candlepin.resource.ConsumerResource=WARN  
log4j.logger.org.candlepin.resource.HypervisorResource=WARN
```

15.2.4. 在 Satellite 上增加日志记录级别

您可以在 `/var/log/foreman/production.log` 中找到 Satellite 的日志。

Satellite 在 Apache 中存储日志：

- `/var/log/httpd/foreman_error.log`
- `/var/log/httpd/foreman_access.log`
- `/var/log/httpd/foreman_ssl_error.log`
- `/var/log/httpd/foreman_ssl_access.log`

流程

1. 在 `/etc/foreman/settings.yaml` 中设置日志级别：

```
:logging:  
:production:  
:type: file  
:layout: pattern  
:level: debug
```

2. 在 `/etc/foreman/settings.yaml` 中启用所选日志记录器：

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

请注意，要查看来自某个区域的日志，必须设置 debug 日志记录。

3.

重启 Satellite 服务：

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

您可以在 `Foreman::Logging.add_loggers` 命令中的 `/usr/share/foreman/config/application.rb` 中找到日志记录器的完整列表。

15.2.5. 为 Qpid Dispatch Router 增加日志记录级别

Qpid 日志到 syslog，可以在 `/var/log/messages` 或 `journalctl` 中查看。在 `/etc/qpid-dispatch/qdrouterd.conf` 中启用 debug 日志记录：

```
enable: debug+
```

确保重启后重启 Qpid Dispatch Router：

```
# systemctl restart qdrouterd
```

小心

运行安装程序将会恢复这个更改。

15.2.6. 为 Qpid Broker 提高日志记录级别

Qpid 日志到 syslog，可以在 `/var/log/messages` 或 `journalctl` 中查看。在 `/etc/qpid/qpidd.conf` 中设置日志级别：

```
log-enable=debug+
```

确保重启后重启 Qpid Broker：

```
# systemctl restart qpidd
```

小心

运行安装程序将会恢复这一更改。

15.2.7. 为 Redis 增加日志记录级别

您可以在 `/var/log/redis/redis.log` 中找到 Redis 的日志。在 `/etc/opt/rh/rh-redis5/redis.conf` 中设置日志级别：

```
loglevel debug
```

确保重启 Redis 服务：

```
# systemctl restart rh-redis5-redis
```

15.2.8. 为 Postgres 增加日志记录级别

您可以在 `/var/lib/pgsql/data/log` 中找到 Postgres 的日志。取消注释 `/var/lib/pgsql/data/postgresql.conf` 中的 `log_statement:`

```
log_statement = 'all'
```

确保重启 Satellite 服务：

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

小心

根据 Satellite 安装的大小，这可能导致磁盘空间非常快。仅在绝对需要时打开此操作。

如需更多调试日志设置，请参阅 [Postgresql 文档](#)。

15.2.9. 为 Satellite 安装程序增加日志记录级别

您可以在 `/var/log/foreman-installer/` 中找到日志文件。在安装过程中增加 Satellite 安装程序的日志级别：

```
# satellite-installer --verbose-log-level debug
```

15.2.10. 为 Pulp 增加日志记录级别

默认情况下, Pulp 日志到 syslog, 可以在 `/var/log/messages` 或 `journalctl` 中查看。在 `/etc/pulp/settings.py` 文件中添加以下配置:

```
LOGGING = {"dynaconf_merge": True, "loggers": {"": {"handlers": ['console'], 'level': 'DEBUG'}}}
```

确保重启 Pulp 服务:

```
# systemctl restart \
pulpcore-api \
pulpcore-content \
pulpcore-resource-manager \
pulpcore-worker@1 \
pulpcore-worker@2 \
rh-redis5-redis
```

15.2.11. 为 Puppet 代理增加日志记录级别

您可以提高卫星服务器上 Puppet 代理的日志级别。

流程

1. 将以下行添加到 `/etc/puppetlabs/puppet/puppet.conf` 文件中的 `[agent]` 块:

```
[agent]
log_level = debug
```

您可以在 `/var/log/puppetlabs/puppet/` 中找到日志

15.2.12. 为 Puppet 服务器增加日志记录级别

您可以提高卫星服务器上 Puppet 服务器的日志级别。

前提条件

- **Puppet 必须在您的 Satellite 中启用。如需更多信息, 请参阅在 Red Hat Satellite 中使用 Puppet 集成管理配置中的启用 Puppet 与 Satellite 集成。**

流程

1. 将以下行添加到 `/etc/puppetlabs/puppet/puppet.conf` 文件中的 `[master]` 块：

```
[master]
log_level = debug
```

2. 重启 Puppet 服务器：

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

您可以在 `/var/log/puppetlabs/puppetserver/` 中找到日志。

15.3. 检索服务的状态

流程

1. 在 Satellite Web UI 中，导航到 **Administer > About**。
2. 在 **Smart Proxies** 选项卡中，您可以查看所有胶囊的状态。
3. 在 **Compute Resources** 选项卡上，您可以查看附加的计算资源提供程序的状态。
4. 在后端 **System Status** 表中，您可以查看所有后端服务的状态。

CLI 过程

- 运行 `hammer ping` 从数据库和 Satellite 服务中获取信息：

```
# hammer ping
```

- 使用 `satellite-maintain` 检查在 `systemd` 中运行的服务的状态：

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


- 使用 `satellite-maintain` 执行健康检查：

```
$ satellite-maintain health check
```

15.4. 重启服务

卫星使用一组后端服务来执行任务。您在 `Satellite` 时遇到问题，检查 `Satellite` 服务的状态。

流程

- 使用 `satellite-maintain` 重启 `Satellite` 服务：

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

提示

运行 `foreman-maintain --help` 了解更多信息。

15.5. 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`。

`background`

从后台处理组件记录信息。

`blob`

用于审计目的的渲染模板的日志内容。

**重要**

blob 日志记录器可能包含敏感数据。

dynflow

从 *Dynflow* 进程记录信息。

ldap

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

notifications

从通知组件记录信息。

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*。

Telemetry

记录来自遥测的调试信息。

templates

记录模板呈现器组件的信息。

流程

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 ldap:true \  
--foreman-loggers sql: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
```

15.6. 配置日志记录到日志或基于文件的日志记录

Satellite 默认使用基于文件的日志记录。您可以使用 `satellite-installer` 命令来重新配置日志记录。

使用日志配置日志的步骤

1.

输入以下 `satellite-installer` 命令，将日志记录配置为 `journald` 服务：

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

2.

可选：要检查日志消息，请使用 `journalctl` 实用程序。例如：

- `journalctl --unit foreman` 和 `journalctl --unit foreman-proxy` 显示 `foreman` 和 `foreman-proxy` 单元的消息
- `journalctl REQUEST=request_ID` 显示指定请求的消息

配置基于文件的日志记录的步骤

1.

输入以下 `satellite-installer` 命令来配置基于文件的日志记录：

```
# satellite-installer \
--reset-foreman-logging-layout \
--reset-foreman-logging-type \
--reset-foreman-proxy-log
```

2.

可选：要检查日志消息，请查看这些文件：

- `/var/log/foreman/production.log`
- `/var/log/foreman-proxy.log`

其他资源

有关日志的更多信息，请参阅 [Red Hat Enterprise Linux 8 配置系统设置指南中的使用命令行查看日志](#)。

15.7. 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 15.1. 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
<code>/var/log/candlepin</code>	订阅管理
<code>/var/log/foreman-installer</code>	安装程序
<code>/var/log/foreman-maintain</code>	Foreman 维护
<code>/var/log/foreman-proxy</code>	Foreman 代理
<code>/var/log/foreman</code>	Foreman
<code>/var/log/httpd</code>	Apache HTTP 服务器
<code>/var/log/messages</code>	各种其他日志消息
<code>/var/log/puppetlabs/puppet</code>	配置管理
<code>/var/log/rhsm</code>	订阅管理
<code>/var/log/tomcat</code>	Candlepin webservice 日志

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。

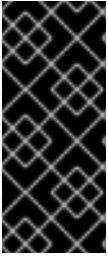
15.8. COLLECTING 日志信息的工具

您可以从日志文件收集信息以对 `Satellite` 进行故障排除。

`sosreport`

`sosreport` 命令从 Linux 系统收集配置和诊断信息，如运行内核版本、载入的模块、运行服务以及系统和配置服务文件。此输出存储在位于 `/var/tmp/sosreport-XXX-20171002230919.tar.xz` 的 tar

文件中。如需更多信息，请运行 `sosreport --help` 或查看 [sosreport 是什么以及如何创建?](#)



重要

集合过程会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。

15.9. 系统日志元数据

下表列出了 `journald` 服务在 `Satellite` 中使用的元数据。您可以使用此元数据来过滤查询。

表 15.2. 系统日志元数据

Name	描述
AUDIT_ACTION	执行的审计操作 示例：创建、更新或删除
AUDIT_TYPE	Audit 资源类型 示例：Host、Subnet 或 ContentView
AUDIT_ID	审计资源数据库 ID 作为数字
AUDIT_ATTRIBUTE	audit 资源字段或更新的数据库列
AUDIT_FIELD_OLD	更新操作的旧审计值
AUDIT_FIELD_NEW	更新操作的新审计值
AUDIT_ID	记录审计主题的数据库 ID
AUDIT_ATTRIBUTE	执行操作的属性名称或列 示例：描述或描述
EXCEPTION_MESSAGE	错误信息被记录时的异常
EXCEPTION_CLASS	记录错误时的 Ruby 类
EXCEPTION_BACKTRACE	当记录错误时，后端作为多行字符串异常
LOC_ID	位置数据库 ID

Name	描述
LOC_NAME	位置名称
LOC_LABEL	位置标签
LOGGER	<p>日志记录器名称</p> <p>要查看默认启用的日志记录器的当前列表，请输入以下命令：</p> <pre># awk '/add_loggers/,/^\$/' /usr/share/foreman/config/application.rb</pre>
ORG_ID	机构数据库 ID
ORG_NAME	机构名称
ORG_LABEL	机构标签
REMOTE_IP	客户端的远程 IP 地址
REQUEST (请求)	由 Action Dispatch 模块生成的请求 ID
会话	为每个会话生成的随机 ID 或无会话请求请求
TEMPLATE_NAME	模板名称
TEMPLATE_DIGEST	渲染模板内容的摘要(SHA256)
TEMPLATE_HOST_NAME	渲染模板的主机名（如果存在）
TEMPLATE_HOST_ID	存在时呈现模板的主机数据库 ID
USER_LOGIN	用户登录名称

第 16 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、提升和同步。

16.1. 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。

在 Satellite Web UI 中，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 16.1. 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	在最后报告间隔期间检测到错误的主机。
	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	在最后报告间隔期间没有收集到任何报告的主机。
	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

Satellite 中所有内容视图的列表及其发布状态。

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 16.2. 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	有有效权限且使用其全部权限的主机。

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 16.3. 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	在调度间隔期间收到无错误的报告。

状态	描述
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。

16.1.1. 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. 在 Satellite Web UI 中，导航到 **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. 在 Satellite Web UI 中，导航到 **Administer > Settings**。
2. 在搜索框中输入 `check_services_before_actions`，然后单击 **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. 点击 **Save**。

16.2. 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. 在 **Satellite Web UI** 中，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。

16.3. 监控 SATELLITE 服务器

审计记录会列出 **Satellite** 上所有用户所做的更改。此信息可用于维护和故障排除。

流程

1. 在 **Satellite Web UI** 中，导航到 **Monitor > Audits** 来查看审计记录。

2.

要获取所有审计属性的列表，请使用以下命令：

```
# foreman-rake audits:list_attributes
```

16.4. 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。

16.4.1. 查看常规胶囊信息

在卫星 Web UI 中，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** 名称以查看详细信息。在 **Overview** 选项卡中，您可以找到与 **Capsule** 表中相同的信息。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可用存储空间？

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。

16.4.2. 监控服务

在 Satellite Web UI 中，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。更多信息请参阅 [第 16.4.3 节“监控 Puppet”](#)。

16.4.3. 监控 Puppet

在 Satellite Web UI 中，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。**



注意

只有在 Satellite 中启用了 Puppet 时，才会使用 Puppet 和 Puppet CA 选项卡。如需更多信息，请参阅在 Red Hat [Satellite 中使用 Puppet 集成管理配置中的启用 Puppet 与 Satellite 集成](#)。

第 17 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](#)。

17.1. 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的结果。

17.2. 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
```
- 可选：您可以使用以下命令安装 `CLI` 插件：

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

17.3. 创建 WEBHOOK 模板

`Webhook` 模板用于在触发 `webhook` 时将 HTTP 请求正文生成到配置的目标。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 > Webhook 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。如果某些事件，可以缺少 @object。您可以确定哪些数据实际上可通过 @payload 变量使用。

有关更多信息，请参阅 **管理主机** 中的 [编写参考的模板](#) 和可用的模板宏和方法，请访问 **Satellite 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**。

17.4. 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，导航到 **Administer > Webhooks**。
2. 点 **Create new**。
3. 从 **Subscribe to** 列表选择一个事件。
4. 输入 **webhook** 的名称。
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**。
6. 单击 **Template** 以选择模板。**Webhook** 模板用于在触发 **Webhook** 时向 **Satellite** 服务器生成 **HTTP** 请求正文。
7. 输入 **HTTP** 方法。
8. 可选：如果您不希望在创建 **Webhook** 时激活 **Webhook**，请取消选择 **Enabled** 标志。
9. 点 **Credentials** 选项卡。
10. 可选：如果需要 **HTTP** 身份验证，请输入 **User and Password**。
11. 可选：如果您不想根据系统证书存储或 **Satellite CA** 验证服务器证书，请取消检查 **验证 SSL**。
12. 在 **Additional** 选项卡中，输入 **HTTP Content Type**。例如，您定义的有效负载上的 **application/json**、**application/xml** 或 **text/plain**。应用程序不会试图转换内容以匹配指定的内容类型。
13. 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 webhook 时，必须分配 SELinux 端口，请参阅配置 SELinux 以保证在连接网络环境中安装卫星服务器中的自定义端口的访问权限。

17.5. 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 & gt; 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	已成功提升内容视图。	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
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

事件名称	描述	payload
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
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)。

事件名称	描述	payload
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	在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

17.6. SHELLHOOKS

使用 Webhook 时，您只能将一个 Satellite 事件映射到一个 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，您可以将 webhook 配置为到达 Capsule API，以运行预定义的 shellhook。shellhook 是一个可执行脚本，只要它可以执行，就可以使用任何语言编写。例如，shellhook 可以包含命令或编辑文件。

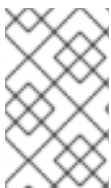
您必须将可执行脚本放在 `/var/lib/foreman-proxy/shellhooks` 中，且只有字母数字字符和下划线的名称。

您可以通过 Webhook 有效负载将输入传递给 shellhook 脚本。此输入重定向到 shellhook 脚本的标

准输入。您可以使用 HTTP 标头将参数传递给 `shellhook` 脚本，格式为 `X-Shellhook-Arg-1` 到 `X-Shellhook-Arg-99`。有关将参数传递给 `shellhook` 脚本的更多信息，请参阅：

- [第 17.8 节“使用 Webhook 将参数传递给 Shellhook 脚本”](#)
- [第 17.9 节“使用 Curl 将参数传递给 Shellhook 脚本”](#)

HTTP 方法必须是 POST。示例 URL 为：
https://capsule.example.com:9090/shellhook/My_Script。



注意

与 `shellhooks` 目录不同，URL 必须包含 `/shellhook/`（以 `singular` 为单位）。

您必须为每个连接到 `shellhook` 的 `webhook` 启用 Capsule 授权，使其能够授权调用。

标准输出和标准错误输出分别作为具有调试或警告级别的消息重定向到 Capsule 日志。

`shellhook` HTTPS 调用不会返回值。

有关创建 `shellhook` 脚本的示例，请参阅 [第 17.10 节“创建 Shellhook 以打印参数”](#)。

17.7. 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
```

17.8. 使用 WEBHOOK 将参数传递给 SHELLHOOK 脚本

使用此流程使用 Webhook 将参数传递给 `shellhook` 脚本。

流程

- 在创建 Webhook 时，在 **Additional** 选项卡中，以以下格式创建 HTTP 标头：

```
{
  "X-Shellhook-Arg-1": "VALUE",
  "X-Shellhook-Arg-2": "VALUE"
}
```

确保标头具有有效的 JSON 或 ERB 格式。仅传递不包含新行或带引号字符的数据库 ID、名称或标签等安全字段。

如需更多信息，请参阅 [第 17.4 节“创建 Webhook”](#)。

示例

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

17.9. 使用 CURL 将参数传递给 SHELLHOOK 脚本

使用 curl 将参数传递给 shellhook 脚本。

流程

- 使用 curl 执行 shellhook 脚本时，以以下格式创建 HTTP 标头：

```
"X-Shellhook-Arg-1: VALUE"
"X-Shellhook-Arg-2: VALUE"
```

示例

```
# curl -sX POST -H 'Content-Type: text/plain' \
```

```
-H "X-Shellhook-Arg-1: Version 1.0" \  
-H "X-Shellhook-Arg-2: My Content View" \  
--data "" https://capsule.example.com:9090/shellhook/My_Script
```

17.10. 创建 SHELLHOOK 以打印参数

创建一个简单的 `shellhook` 脚本，该脚本在运行远程执行作业时打印“Hello World!”。

前提条件

- 已安装 `webhook` 和 `shellhooks` 插件。如需更多信息，请参阅：
 - [第 17.2 节“安装 Webhook”](#)
 - [第 17.7 节“安装 Shellhooks 插件”](#)

流程

1. 修改 `/var/lib/foreman-proxy/shellhooks/print_args` 脚本，以将参数打印到标准错误输出，以便您可以在 `Capsule` 日志中看到它们：

```
#!/bin/sh  
#  
# Prints all arguments to stderr  
#  
echo "$@" >&2
```

2. 在 `Satellite Web UI` 中，导航到 `Administer > Webhooks`。
3. 点 `Create new`。
4. 从 `Subscribe to` 列表中，选择 `Actions Remote Execution Run Host Job Succeeded`。

5. 输入 **webhook** 的名称。
6. 在 **Target URL** 字段中，输入您的 **Capsule** 服务器的 URL，后跟 **:9090/shellhook/print_args**：

```
https://capsule.example.com:9090/shellhook/print_args
```

请注意，URL 中的 **shellhook** 是单数的，这与 **shellhooks** 目录不同。

7. 从 **Template** 列表中，选择 **Empty Payload**。
8. 在 **Credentials** 选项卡上，选中 **Capsule Authorization**。

9. 在 **Additional** 选项卡中，在 **Optional HTTP headers** 字段中输入以下文本：

```
{
  "X-Shellhook-Arg-1": "Hello",
  "X-Shellhook-Arg-2": "World!"
}
```

10. 点 **Submit**。现在，您已成功创建了一个 **shellhook**，它会在每次远程执行作业都成功时将 **"Hello World!"** 打印到 **Capsule** 日志。

验证

1. 在任何主机上运行远程执行作业。您可以使用 **时间** 作为命令。如需更多信息，请参阅 [管理主机中的执行远程作业](#)。
2. 验证 **shellhook** 脚本是否已触发，并将 **"Hello World!"** 输出到 **Capsule** 服务器日志：

```
# tail /var/log/foreman-proxy/proxy.log
```

您应该在日志末尾找到以下行：

```
[!] Started POST /shellhook/print_args
```

```
[!] Finished POST /shellhook/print_args with 200 (0.33 ms)
[!] [3520] Started task /var/lib/foreman-proxy/shellhooks/print_args\ Hello\ World!
[W] [3520] Hello World!
```

第 18 章 搜索和书签

卫星在 **Satellite Web UI** 的大部分页面中提供强大的搜索功能。它可让您搜索 **Satellite** 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。

18.1. 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 18.2 节“使用可用文本搜索”](#)。

18.1.1. 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](#)。

18.1.2. 查询 Operator

下表中列出了可在 **parameter** 和 **value** 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 18.1. 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		

Operator	短名称	描述	示例
>	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		
^	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。 在仪表板上没有 hostgroup 或 null? hostgroup ，它带有主机概述，搜索将返回没有分配的主机组的所有主机。
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 18.2. 搜索接受的逻辑 Operator

Operator	其它通知		示例
和	&	&&	<code><whites pace></code> class = motd AND environment ~ production
或			errata_status = errata_needed errata_status = security_needed
not	-	!	hostgroup ~ rhel7 not status.failed

18.1.3. 查询值

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。

18.2. 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。

18.3. 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。

18.3.1. 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。

流程

1. 在卫星 Web UI 中，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 **Search** 按钮右侧的箭头，然后选择 **Bookmark this search**。
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，将书签设置为公共复选框，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。

18.3.2. 删除书签

您可以在“书签”页面中删除书签。

流程

1. 在 **Satellite Web UI** 中，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. 管理设置

本节包含您可以在 *Satellite Web UI* 中编辑的设置的设置的信息，方法是导航到 **Administer > Settings**。

A.1. 常规设置

设置	默认值	描述
管理员电子邮件地址		默认管理员电子邮件地址
Satellite URL		Satellite 实例可以访问的 URL。另请参阅 Provisioning > Unattended URL 。
每个页的条目	20	Satellite 中每个页面显示的记录数
修复 DB 缓存	否	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。
DB 待定	否	foreman-rake db:seed 在下次安装程序模块上是否执行？
胶囊请求超时	60	打开并读取从 Satellite 到 Capsule（以秒为单位）的 HTTP 请求的超时。
登录页页脚文本		要在登录页面页中显示的文本。
显示主机电源状态	是	显示主机索引页面上的电源状态。此功能调用计算资源提供商可能会降低主机列表页面上的性能。
HTTP(S)代理		为 Satellite 产品传出 HTTP(S)连接设置代理。必须在操作系统级别上配置系统范围的代理。
HTTP(S)代理（主机外）	[]	设置请求不会代理的主机名。默认排除对本地主机的请求。
显示实验室	否	是否显示菜单来访问实验实验功能（需要重新加载页面）。
将域名附加到主机	是	如果设置为 Yes ，Satellite 在置备新主机时附加域名。

设置	默认值	描述
不同步间隔	30	受管主机定期报告，如果报告间隔超过此持续时间，则主机被视为不同步。您可以通过添加 outofsync_interval 参数（每个主机为 Hosts > All hosts > \$host > Edit > Add Parameter）来覆盖主机上的这个值。
Satellite UUID		Satellite 实例 ID。唯一标识 Satellite 实例。
默认语言		新用户的 UI 会使用此语言。
默认时区		用于新用户的时区。
实例标题		顶部导航栏上显示了实例标题（需要重新加载页面）。
保存的审计间隔		保留审核数据的持续时间（以天为单位）。保留空来禁用审计清理。
新主机详情 UI	是	卫星为主机详情加载新的 UI。

A.2. SATELLITE 任务设置

设置	默认值	描述
同步任务超时	120	在引发异常前等待同步任务完成的秒数。
启用 dynflow 控制台	是	启用 dynflow 控制台 (/foreman_tasks/dynflow) 进行调试。
对于 dynflow 控制台需要 auth	是	在访问 dynflow 控制台前，用户必须以管理权限的身份进行身份验证。
Capsule action 重试计数	4	失败前，允许在胶囊上启动任务的次数。
Capsule action 重试间隔	15	重试之间的时间（以秒为单位）。
允许放置批处理任务	是	在胶囊上启用批触发任务。
胶囊任务批量大小	100	如果启用了 foreman_tasks_proxy_batch_trigger ，一个请求中包含的任务数量。

设置	默认值	描述
任务故障排除 URL		指向任务故障排除文档的 URL。它应包含一个使用规范化任务标签替换的 <code>%{label}</code> 占位符（仅限于字母数字字符）。也可以使用 <code>%{version}</code> 占位符。
轮询间隔乘以的倍数	1	轮询倍数，用于乘以默认轮询间隔。您可以使用它来防止对长时间运行的任务进行轮询。

A.3. 模板同步设置

设置	默认值	描述
"关联"	New	将模板与操作系统、机构和位置相关联。
分支		Git 存储库中的默认分支。
提交消息	Satellite 用户提供的模板导出	用于导出的模板的自定义提交消息。
dirname	/	包含模板的 Git 存储库中的目录。
Filter		导入或导出与此正则表达式匹配的名称。不区分大小写。代码段不会被过滤。
强制导入	否	如果设置为 Yes ，则导入过程中将覆盖锁定的模板。
锁定模板	keep, 不要锁定新的	如何处理导入模板的锁定。
元数据导出模式	刷新	默认元数据导出模式。 可能的选项： 刷新 重新渲染元数据。 保留现有 元数据。 删除 在没有元数据的情况下导出模板。
negate	否	negate 用于导入或导出的过滤器。
prefix		添加了一个字符串作为导入模板的前缀。

设置	默认值	描述
仓库		<p>从中导入或导出模板的目标路径。可以使用不同的协议，例如：</p> <p>/tmp/dir</p> <p>git://example.com</p> <p>https://example.com</p> <p>ssh://example.com</p> <p>当导出到 /tmp 时，请注意生产部署可能配置为使用 私有 tmp。</p>
详细程度	否	选择 Rake 任务导入模板的详细程度。

A.4. 发现的设置

设置	默认值	描述
发现位置		表示将发现的主机放入的默认位置。
发现机构		表示将发现的主机添加到的默认组织。
接口事实	discovery_bootif	用于主接口检测的事实名称。
创建绑定接口	否	如果在使用 LLDP 在同一 VLAN 中检测到另一个接口，则自动创建绑定接口。
清理所有事实	否	在置备过程中清理所有报告的事实（发现事实除外）。
主机名事实	discovery_bootif	用于主机名的事实列表(comma separated, first wins)。
自动置备	否	使用置备规则自动置备新发现的主机。
重启	是	在置备过程中自动重启或 kexec 发现的主机。
主机名前缀	mac	用于主机名的默认前缀。必须以字母开头。
事实列		要在主机列表中显示的额外事实列（减去分隔）。

设置	默认值	描述
突出显示的事实		用于整理亮点事实的正则表达式 - 例如 <code>^(abc cde)\$</code> 。
存储事实		正则表达式，用于组织存储部分的事实。
软件事实		正则表达式，用于组织软件部分的事实。
硬件事实		正则表达式，用于组织硬件部分的事实。
网络事实		正则表达式，用于组织网络部分的事实。
IPMI 事实		正则表达式，用于组织 <i>智能平台管理接口</i> (IPMI)部分的事实。
锁定 PXE	否	自动生成 <i>预启动执行环境</i> (PXE)配置，以固定新发现的主机以进行发现。
锁定的虚拟机模板名称	pxelinux_discovery	在将主机固定到发现时，要使用的 PXELinux 模板。
锁定 PXEGrub 模板名称	pxegrub_discovery	将主机固定为发现时使用的 PXEGrub 模板。
锁定 PXEGrub2 模板名称	pxegrub2_discovery	将主机固定为发现时使用的 PXEGrub2 模板。
强制 DNS	是	置备发现的主机时强制创建 DNS 条目。
现有 NIC 时出错	否	不要允许发现与置备 <i>网络接口卡</i> (NIC) (早期错误)的 MAC 匹配的现有受管主机。
名称生成器类型	事实 + 前缀	发现主机命名模式。
首选 IPv6	否	调用发现节点时，首选 IPv6 到 IPv4。

A.5. 引导磁盘设置

设置	默认值	描述
iPXE directory	<code>/usr/share/ipxe</code>	包含 iPXE 镜像的目录路径。
ISOLINUX 目录	<code>/usr/share/syslinux</code>	包含 ISOLINUX 镜像的目录路径。
SYSLINUX 目录	<code>/usr/share/syslinux</code>	包含 SYSLINUX 镜像的目录路径。

设置	默认值	描述
Grub2 目录	<code>/var/lib/tftpboot/grub2</code>	包含 <code>grubx64.efi</code> 和 <code>shimx64.efi</code> 的目录路径。
主机镜像模板	引导磁盘 iPXE - 主机	用于特定于主机的引导磁盘的 iPXE 模板。
通用镜像模板	引导磁盘 iPXE - 通用主机	用于通用主机引导磁盘的 iPXE 模板。
通用 Grub2 EFI 镜像模板	引导磁盘 Grub2 EFI - 通用主机	Grub2 模板，用于通用 <i>可扩展固件接口</i> (EFI) 主机引导磁盘。
ISO 生成命令	<code>genisoimage</code>	要生成 ISO 镜像的命令，使用 <code>genisoimage</code> 或 <code>mkisofs</code> 。
安装介质缓存	是	为完整主机镜像缓存安装介质文件。
允许的 bootdisk 类型	<code>[generic, host, full_host, subnet]</code>	允许的引导磁盘类型列表。留空以将其留空。

A.6. RED HAT CLOUD SETTINGS

设置	默认值	描述
自动清单上传	是	启用自动将主机清单上传到红帽云。
自动同步建议	否	启用从红帽云自动同步智能分析工具建议。
模糊主机名	否	模糊处理发送到红帽云的主机名。
模糊处理主机 ipv4 地址	否	发送到红帽云的模糊 IPv4 地址。
RHC 守护进程的 ID	*****	RHC 守护进程 ID。

A.7. 内容设置

设置	默认值	描述
默认 HTTP 代理		用于同步内容的默认 HTTP 代理服务器。
CDN SSL 版本		用于与 CDN 通信的 SSL 版本。
默认同步操作系统置备模板	Kickstart 默认	从同步内容中创建的操作系统的默认置备模板。

设置	默认值	描述
默认同步操作系统完成模板	Kickstart 默认完成	从同步内容创建的新操作系统的默认完成模板。
默认同步 OS 用户数据	Kickstart 默认用户数据	从同步内容创建的新操作系统的默认用户数据。
默认同步 OS PXELinux 模板	Kickstart default PXELinux	从同步内容创建的新操作系统的默认 PXELinux 模板。
默认同步操作系统 PXEGrub 模板	Kickstart 默认 PXEGrub	从同步内容创建的新操作系统的默认 PXEGrub 模板。
默认同步操作系统 PXEGrub2 模板	Kickstart 默认 PXEGrub2	从同步内容创建的新操作系统的默认 PXEGrub2 模板。
默认同步操作系统 iPXE 模板	Kickstart 默认 iPXE	从同步内容创建的新操作系统的默认 iPXE 模板。
默认同步操作系统分区表	Kickstart 默认	从同步内容中创建的新操作系统的默认分区表。
默认同步 OS kexec 模板	发现红帽 kexec	从同步内容中创建的新操作系统的默认 kexec 模板。
默认同步操作系统 Atomic 模板	Atomic Kickstart 默认	用于从同步内容创建的新原子操作系统的默认置备模板。
清单刷新超时	1200	刷新清单时的超时（以秒为单位）。
接受操作超时	20	等待主机获取远程操作的时间（以秒为单位）。
完成操作超时	3600	等待主机完成远程操作的时间（以秒为单位）。
启用订阅连接	是	可以与红帽门户通信以获取订阅。
从内容视图安装勘误表	否	仅根据主机的内容视图和生命周期环境中的勘误表来计算勘误表主机状态。
限制 Composite Content View promotion	否	如果启用此项，则无法发布或提升复合内容视图，除非它在目标环境中存在它中包含的内容视图。
在操作前检查服务	是	在执行操作前，检查 pulp 和 candlepin 等后端服务的状态？

设置	默认值	描述
用于同步存储库的批量大小	100	应在胶囊上同步多少个存储库。较小的数字可能会导致同步时间更长。较大的数字会增加 dynflow 负载。
在内容视图提升后同步胶囊	是	在内容视图提升后是否自动同步 Capsule。
默认自定义存储库下载策略	immediate	自定义存储库的默认下载策略。 immediate 或 on_demand 。
默认 Red Hat Repository 下载策略	on_demand	启用红帽软件仓库的默认下载策略。 immediate 或 on_demand 。
默认胶囊下载策略	on_demand	胶囊同步的默认下载策略。 继承、立即 或 on_demand 。
Pulp 导出目标文件路径	/var/lib/pulp/katello-export	用于导出的存储库的磁盘位置。
Pulp 3 导出目标文件路径	/var/lib/pulp/exports	对 Pulp 3 导出的存储库的磁盘位置。
Pulp 客户端密钥	/etc/pki/katello/private/pulp-client.key	用于 Pulp 服务器身份验证的 SSL 密钥路径。
Pulp 客户端证书	/etc/pki/katello/certs/pulp-client.crt	用于 Pulp 服务器身份验证的 SSL 证书路径。
同步连接超时	300	同步时连接的总超时（以秒为单位）。
默认使用远程执行	否	如果启用，则使用远程执行而不是 katello-agent 用于远程操作。
在取消注册时删除主机	否	使用 subscription-manager 取消注册主机时，也会删除主机记录。也可以删除链接到虚拟机和 DNS 记录等主机的受管资源。
订阅管理器名称注册事实		使用 subscription-manager 注册主机时，强制将指定的事实用作主机名（ fact.fact 的形式）。
订阅管理器名称注册事实严格匹配	否	如果启用了此操作，并且设置了 register_hostname_fact 并提供，注册仅使用该事实来按照名称查找新主机，并跳过所有主机名匹配。
默认位置订阅的主机	默认位置	注册后存储了新订阅主机的默认位置。

设置	默认值	描述
过期日	120	在提醒续订前，在订阅中剩余天数。
Content View Dependency Solving Default	否	默认依赖项解决了新内容视图的值。
主机字典 DMI UUID	[]	如果因为重复的 桌面管理接口(DMI)UUID 而无法注册主机，请在此处添加用逗号分开的值。后续注册为受影响的主机生成唯一的 DMI UUID。
Host Profile Assume	是	启用新主机注册，假设带有匹配主机名注册的配置集，只要另一台主机没有使用 DMI UUID。
主机配置文件可在构建中更改	否	启用主机注册以绕过 Host Profile Assume ，只要主机处于构建模式。
仅在构建中注册主机	否	仅在处于构建模式时启用主机重新注册。
主机任务 workers 池大小	5	池中用于处理主机相关任务的 worker 数量。当设置为 0 时，会使用默认队列。需要重启 dynflowd/foreman-tasks 服务。
适用容量批处理大小	50	每个任务要处理的主机适用性计算数量。
Autosearch	是	对于支持它的页面，在搜索输入中键入时会自动执行搜索。
Autosearch delay	500	如果启用了 Autosearch，在键入时执行搜索前以毫秒的延迟。
Pulp 批量负载大小	2000	从单个页面 Pulp API 调用中获取的项目数量。
在没有 Dynflow 的情况下上传配置集	是	启用 Katello 以更新主机已安装的软件包、启用的存储库和模块清单直接嵌套在 Dynflow 任务中（如果 Puma 进程使用太多内存，则尝试关闭）。
孤立的内容保护时间	1440	以分钟为单位将孤立内容视为孤立的时间。
首选通过 Capsule 注册以进行远程执行	否	首选使用使用主机在远程执行时注册的代理。

设置	默认值	描述
允许删除已发布的内容视图中的存储库	是	启用删除用户之前在一个或多个 Content View 版本中发布的存储库。

A.8. 身份验证设置

设置	默认值	描述
OAuth 活跃	是	卫星将使用 OAuth 进行 API 授权。
OAuth 消费者密钥	*****	OAuth 消费者密钥。
OAuth 消费者机密	*****	OAuth 消费者机密。
OAuth 映射用户	否	Satellite 根据 request-header 中的用户名映射用户。如果禁用，OAuth 请求具有管理员权限。
失败登录尝试限制	30	Satellite 会阻止用户在指定失败登录尝试后 5 分钟内从传入的 IP 地址登录。设置为 0 以禁用 brute 强制保护。
限制已注册的胶囊	是	只有已知胶囊才能访问使用胶囊身份验证的功能。
capsule 需要 SSL	是	客户端 SSL 证书用于标识胶囊（： <code>:require_ssl</code> 还应启用）。
可信主机	[]	除了 Capsule 之外，访问事实/报告导入器和 ENC 输出外要信任的主机名、IPv4、IPv6 地址或子网的列表。
SSL 证书	<code>/etc/foreman/client_cert.pem</code>	Satellite 用于与其代理通信的 SSL 证书路径。
SSL CA 文件	<code>/etc/foreman/proxy_ca.pem</code>	Satellite 用于与其代理通信的 SSL CA 文件路径。
SSL 私钥	<code>/etc/foreman/client_key.pem</code>	Satellite 用于与其代理通信的 SSL 私钥路径。
SSL 客户端 DN 环境	HTTP_SSL_CLIENT_S_DN	包含来自客户端 SSL 证书的主题 DN 的环境变量。
SSL 客户端验证 env	HTTP_SSL_CLIENT_VERIFY	包含客户端 SSL 证书的验证状态的环境变量。

设置	默认值	描述
SSL 客户端证书 env	HTTP_SSL_CLIENT_CERT	包含客户端 SSL 证书的环境变量。
服务器 CA 文件		模板中使用的 SSL CA 文件路径来验证与 Satellite 的连接。
Websocket SSL 密钥	etc/pki/katello/private/katello-apache.key	Satellite 加密 websocket 的私钥文件路径。
Websocket SSL 证书	/etc/pki/katello/certs/katello-apache.crt	Satellite 用于加密 websocket 的证书路径。
websocket 加密	是	VNC/SPICE websocket 代理控制台访问加密（需要 websockets_ssl_key/cert 设置）。
登录委托注销 URL		在注销时将您的用户重定向到此 URL。同时启用 授权登录委托 。
授权登录委托身份验证源用户 autcreate	外部	创建外部经过身份验证的用户的外部身份验证源的名称（请参阅 授权登录委托 ）。空意味着没有自动创建。
授权登录委托	否	使用 REMOTE_USER HTTP 标头授权登录委托。
授权登录委托 API	否	使用 REMOTE_USER HTTP 标头为 API 调用授权登录委托。
闲置超时	60	在指定数分钟后注销闲置用户。
bcrypt 密码成本	9	内部 auth-sources 的 bcrypt password hash 功能的成本值(4TOKEN-方式30)。数值越安全，但验证速度较慢，特别是用于无状态 API 调用和 UI 登录的情况。需要更改密码才能影响现有密码。
BMC 凭证访问权限	是	允许通过 ENC YAML 输出和模板中的 BMC 接口密码访问 BMC 接口密码。
OIDC JWKS URL		OpenID Connect <i>JSON Web Key Set</i> (JWKS)URL.通常 ， https://keycloak.example.com/auth/realms/<realm name>/protocol/openid-connect/certs 使用 Keycloak 作为 OpenID 供应商。

设置	默认值	描述
OIDC Audience	[]	用于身份验证的 OpenID Connect Audience 的名称。对于 Keycloak, 这是客户端 ID。
OIDC Issuer		签发 <i>JSON Web 令牌</i> (JWT)的主体, 该主体在大多数 OpenID 供应商中都存在 /.well-known/openid-configuration 。
OIDC 算法		在 OpenID 提供程序中编码 JWT 的算法。

A.9. 电子邮件设置

设置	默认值	描述
电子邮件回复地址		Satellite 发送的电子邮件的电子邮件地址。
电子邮件主题前缀		添加到所有传出电子邮件的前缀。
发送欢迎电子邮件	否	向新用户发送包括用户名和 URL 的欢迎电子邮件。
交付方法	sendmail	用于发送电子邮件的方法。
SMTP 启用 StartTLS auto	是	SMTP 自动启用 StartTLS。
SMTP OpenSSL 验证模式	默认验证模式	使用 TLS 时, 您可以设置 OpenSSL 如何检查证书。
SMTP 地址		要连接的 SMTP 地址。
SMTP 端口	25	要连接的 SMTP 端口。
SMTP HELO/EHLO 域		HELO/EHLO 域。
SMTP 用户名		用于进行身份验证的用户名 (如果需要)。
SMTP 密码	*****	用于进行身份验证的密码 (如果需要)。
SMTP 身份验证	none	如果需要, 指定身份验证类型。

设置	默认值	描述
Sendmail 参数	-i	为 sendmail 指定附加选项。仅在发送方法设为 sendmail 时使用。
Sendmail 位置	/usr/sbin/sendmail	sendmail 可执行文件的位置。仅在发送方法设为 sendmail 时使用。

A.10. 通知设置

设置	默认值	描述
RSS 启用	是	拉取 RSS 通知。
RSS URL	https://www.redhat.com/en/rss/blog/channel/red-hat-satellite	从中获取 RSS 通知的 URL。

A.11. 置备设置

设置	默认值	描述
主机所有者		置备的主机上的默认所有者（如果为空的 Satellite 将使用当前用户）。
root 密码	*****	置备的主机上的默认加密根密码。
无人值守 URL		主机在构建期间从获取模板的 URL。当它以 https、无人值守或用户数据开头时，控制器无法使用 HTTP 进行访问。
Safemode rendering	是	<p>启用置备模板的安全模式渲染。默认和推荐的选项是 拒绝访问 变量以及任何未列在 Satellite 中的对象。</p> <p>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。这不是安全选择，特别是在大型公司中。</p>
在没有构建的情况下以无人值守方式访问	否	启用在不使用构建模式的情况下访问无人值守 URL。

设置	默认值	描述
查询本地名称服务器	否	Satellite 查询本地配置的解析器而不是 SOA/NS 权威。
安装令牌生命周期	360	安装令牌应有效的时间（以分钟为单位）。设置为 0 以禁用令牌。
SSH 超时	120	SSH 置备超时前的时间（以秒为单位）。
libvirt 默认控制台地址	0.0.0.0	在使用 libvirt 置备新虚拟机时，应用于控制台的 IP 地址。
从构建请求更新 IP	否	卫星使用发出构建请求的 IP 更新主机 IP。
为虚拟机使用简短名称	否	Satellite 使用短主机名而不是 FQDN 来创建新虚拟机。
DNS 超时	[5, 10, 15, 20]	DNS 查找尝试尝试超时（以秒为单位）列表，如 dns_lookup 宏和 DNS 记录冲突验证。
清理失败的部署	是	如果调配脚本以非零退出代码结尾，则 Satellite 会删除虚拟机。
名称生成器类型	Random-based	<p>指定在创建新主机时用于生成主机名的方法。</p> <p>基于默认 Random 的 选项会生成一个唯一的随机主机名，但您不必使用。这对创建多个主机并不知道如何命名主机的用户很有用。</p> <p>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以及希望他们始终获得同一主机名的用户很有用。</p> <p>Off 选项禁用名称生成器函数，并将 hostname 字段留空。</p>
默认 PXE 全局模板条目		全局模板中的默认 PXE 菜单项 - 本地 、 发现 或 自定义 ，在模板 default 中使用空白。
默认 PXE 本地模板条目		本地模板中的默认 PXE 菜单项 - 本地 、 local_chain_hd0 或 自定义 ，将空白用于模板 default。
iPXE 中间脚本	iPXE 中间脚本	用于无人值守安装的中间 iPXE 脚本。

设置	默认值	描述
销毁 host delete 上的关联虚拟机	否	销毁 host delete 上的关联虚拟机。启用后，连接到主机的虚拟机在计算资源上被删除。禁用后，主机被删除后，虚拟机将取消链接，即它们保留在计算资源上，并可重新关联或导入到卫星。这不会自动关闭虚拟机
最大结构化事实	100	结构化子树中的最大键数，该统计数据存储在 satellite::dropped_subtree_facts 中。
默认全局注册模板	全局注册	全球注册模板。
默认"主机初始配置"模板	Linux host_init_config 默认	创建新操作系统时自动分配默认"主机初始配置"模板。
全局默认 PXEGrub2 模板	PXEGrub2 全局默认值	全局默认 PXEGrub2 模板。此模板被部署到所有配置的 TFTP 服务器。它不会受到升级的影响。
全局默认 PXELinux 模板	PXELinux 全局默认值	全局默认 PXELinux 模板。此模板被部署到所有配置的 TFTP 服务器。它不会受到升级的影响。
全局默认 PXEGrub 模板	PXEGrub 全局默认值	全局默认 PXEGrub 模板。此模板被部署到所有配置的 TFTP 服务器。它不会受到升级的影响。
全局默认 iPXE 模板	iPXE 全局默认值	全局默认的 iPXE 模板。此模板被部署到所有配置的 TFTP 服务器。它不会受到升级的影响。
本地引导 PXEGrub2 模板	PXEGrub2 默认本地引导	选择作为本地引导的默认 PXEGrub2 的模板。
本地引导 PXELinux 模板	PXELinux 默认本地引导	选为 local boot 的 PXELinux default 模板。
本地引导 PXEGrub 模板	PXEGrub 默认本地引导	为本地引导选择为 PXEGrub 默认的模板。
本地引导 iPXE 模板	iPXE 默认本地引导	选择为 iPXE default 进行本地引导的模板。
Manage PuppetCA	是	卫星在调配新主机时自动执行证书签名请求。

设置	默认值	描述
证书使用 UUID	否	Satellite 为证书签名使用随机 UUID，而不是主机名。
显示不支持的自定义模板	否	显示不支持的调配模板。启用后，将显示所有可用的模板。禁用后，仅显示红帽支持的模板。

A.12. 事实设置

设置	默认值	描述
上传事实时创建新主机	是	在收到新事实时，Satellite 会创建主机。
位置事实	satellite_location	在 Puppet 运行之后创建的主机放入此事实所指定的位置。
机构事实	satellite_organization	在 Puppet 运行之后创建的主机放置在此事实指定的机构中。事实的内容应该是该组织的完整标签。
默认位置	默认位置	在 Puppet 运行之后创建的主机没有发送位置事实放置在此位置。
默认机构	默认机构	在 Puppet 运行之后创建的主机没有发送组织事实，则将放置在此机构中。
从事实更新主机组	是	卫星从其事实更新主机的主机组。
忽略操作系统的事实	否	停止从事实更新操作系统。
忽略域的事实	否	停止事实中更新域值。
从事实更新子网	无	卫星从主机的事实更新主机子网。
忽略用于置备的接口事实	否	停止从事实更新 IP 和 MAC 地址值（所有接口）。
忽略具有匹配标识符的接口	[lo,en*v*,usb*,vnet*,macvtap*,vdsmdummy,veth*,tap*,qbr*,qv*,qvo*,qr-*,qg-*,vlinuxbr*,vovsbr*,br-int]	跳过创建或更新主机网络接口对象，其标识符与来自传入事实的这些值匹配。您可以使用 * 通配符来匹配索引的标识符，如 macvtap* 。忽略的接口原始事实仍会存储在数据库中，请参阅 Exclude pattern 设置以了解更多详细信息。

设置	默认值	描述
satellite 中存储的事实的排除模式	[lo,en*v*,usb*,vnet*, macvtap*,;vdsmdummy*, veth*,tap*,qbr*,qv*,qvo*, qr-*,qg-*,vlinuxbr*, vovsbr*,br- int,load_averages::*, memory::swap::available *, memory::swap::capacity, memory::swap::used*, memory::system::availab le*, memory::system::capacit y,memory::system::used*, memoryfree,memoryfree_ mb,swapfree,swapfree_m b,uptime_hours,uptime_d ays]	导入的所有事实（Puppet、Ansible、rhsm）的 exclude pattern。这些事实不存储在 satellite 数据库中。您可以使用 * 通配符来匹配带有 indexes 的名称，例如： ignore* 会过滤 ignore、ignore123 以及 a::ignore 或 a::ignore123::b。

A.13. 配置管理设置

设置	默认值	描述
在上传报告时创建新主机	是	收到报告时，Satellite 会创建主机。
Matchers 继承	是	在评估主机组、组织和位置的智能类参数时，卫星匹配器将被子项继承。
默认参数查找路径	[fqdn,hostgroup,os, domain]	默认情况下，Satellite 按此顺序评估主机智能类参数。
参数中的 Interpolate ERB	是	卫星在 ENC 输出中以参数值解析 ERB。
始终显示配置状态	否	所有主机即使没有分配 Puppet 胶囊，也显示配置状态。

A.14. 远程执行设置

设置	默认值	描述
回退到 Any Capsule	否	使用 Remote Execution 搜索任何代理的主机。这在主机没有子网或者子网没有执行代理时很有用。
启用 Global Capsule	是	搜索分配给主机的代理外的远程执行代理。搜索仅限于主机的组织和位置。

设置	默认值	描述
SSH 用户	root	用于 SSH 的默认用户。您可以通过设置 remote_execution_ssh_user 参数覆盖每个主机。
有效用户	root	用于执行脚本的默认用户。如果用户与 SSH 用户不同，则使用 <code>su</code> 或 <code>sudo</code> 切换用户。
有效的用户方法	sudo	用于切换到有效用户的命令。 [sudo,dzdo,su]
有效用户密码	*****	有效用户密码。请参阅 效率用户 。
同步作业模板	是	运行 db:seed 时是否从磁盘同步模板。
SSH 端口	22	用于 SSH 通信的端口。默认端口 22。您可以通过设置 remote_execution_ssh_port 参数来覆盖每个主机。
通过 IP 连接	否	主机接口上的 IP 地址是否优先于 FQDN。当 DNS 没有正确解析 FQDN 时，这很有用。您可以通过设置 remote_execution_connect_by_ip 参数来覆盖每个主机的这个操作。对于双栈主机，请考虑 remote_execution_connect_by_ip_prefer_ipv6 设置。
IPv4 首选 IPv6	否	使用 IP 地址进行连接时，首选 IPv6 地址？如果没有设置 IPv6 地址，它会自动回退到 IPv4。您可以通过设置 remote_execution_connect_by_ip_prefer_ipv6 参数为每个主机覆盖这个操作。默认情况下，对于兼容性，IPv4 优先于 IPv6。
默认 SSH 密码	*****	用于 SSH 的默认密码。您可以通过设置 remote_execution_ssh_password 参数来覆盖每个主机。
默认 SSH 密钥密码短语	*****	用于 SSH 的默认密钥密码短语。您可以通过设置 remote_execution_ssh_key_passphrase 参数来覆盖每个主机。
worker 池大小	5	池中用于处理远程执行作业的 worker 数量。需要重启 dynflowd/satellite-tasks 服务。

设置	默认值	描述
清理工作目录	是	工作目录是否在任务完成后删除。您可以通过设置 remote_execution_cleanup_working_dirs 参数来覆盖每个主机的这个操作。
Cockpit URL		从哪里查找 Web 控制台按钮的 Cockpit 实例。默认情况下不显示任何按钮。
表单作业模板	运行命令 - SSH 默认	选择以作业调用形式预先选择的作业模板。
任务调用报告模板	作业 - Invocation report template	选择一个报告模板，用于为特定远程执行作业生成报告。

A.15. ANSIBLE 设置

设置	默认值	描述
私钥路径		使用此方法提供 Ansible 使用而非密码的 SSH 私钥路径。使用 ansible_ssh_private_key_file 主机参数覆盖。
连接类型	ssh	在运行 Ansible playbook 时默认使用此连接类型。您可以通过添加 ansible_connection 参数来覆盖主机上的这个值。
WinRM 证书验证	validate	在运行 Ansible playbook 时启用或禁用 WinRM 服务器证书验证。您可以通过添加 ansible_winrm_server_cert_validation 参数来覆盖主机上的这个值。
默认详细程度	Disabled	卫星在运行 Ansible playbook 时增加了此级别的详细程度，用于额外的调试输出。
后置备超时	360	设置超时（以秒为单位）来设置在主机完全调配后触发 Ansible 角色任务 playbook 时设置的超时（以秒为单位）。将其设置为您希望主机在重启后完成的最大时间。
Ansible 报告超时	30	主机应报告的时间超时（以分钟为单位）。

设置	默认值	描述
Ansible 没有禁用同步	否	在报告没有达到配置的时间间隔后，禁用主机配置状态会变为不同步 Ansible。
默认 Ansible 清单报告模板	Ansible - Ansible 清单	卫星使用此模板来调度报告与 Ansible 清单。
要忽略的 Ansible 角色	[]	从 Capsule 导入角色时要排除的角色。预期的输入是用逗号分开的值，您可以使用 * 通配符元字符。例如： foo*,*b*,*bar 。
Ansible 的 Capsule 任务批处理大小		如果启用了 satellite_tasks_proxy_batch_trigger ，应对一个请求中发送到胶囊的任务数量。如果设置，它会覆盖 Ansible 作业的 satellite_tasks_proxy_batch_size 设置。