Red Hat Satellite 6.15

在连接的网络环境中安装 Satellite 服务器

在可访问互联网的网络中安装和配置 Satellite 服务器

Last Updated: 2024-06-21

Red Hat Satellite 6.15 在连接的网络环境中安装 Satellite 服务器

在可访问互联网的网络中安装和配置 Satellite 服务器

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

法律通告

摘要

本指南介绍了如何从连接的网络安装 Red Hat Satellite，执行初始配置和配置外部服务。

目录

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。由于这项工作的艰巨性，这些变化正在尽可能地逐步更新。详情请查看 CTO Chris Wright 的信息。

对红帽文档提供反馈

我们感谢您对我们的文档提供的信息。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 为安装准备您的环境

在安装 Satellite 前，请确保您的环境满足以下要求。

1.1. 系统要求

以下要求适用于联网的基本操作系统：

- x86_64 架构
- Red Hat Enterprise Linux 8 的最新版本
- 至少 4 核 2.0 GHz CPU
- Satellite 服务器至少需要 20 GB RAM。另外，还建议至少 4 GB RAM 交换空间。以 RAM 小于最小值运行的 Satellite 可能无法正确运行。
- 唯一的主机名，可以包含小写字母、数字、点(.)和连字符(-)
- 当前 Red Hat Satellite 订阅
- 管理用户(root)访问
- 使用完全限定域名进行全正向和反向 DNS 解析

Satellite 只支持 **UTF-8** 编码。如果您的个人是美国的，并且您的语言是英语，请将 **en_US.utf-8** 设置为系统范围的区域设置。有关在 Red Hat Enterprise Linux 中 配置系统区域设置的更多信息，请参阅 配置系统本地指南。

您的 Satellite 必须在您的客户门户网站中有 Red Hat Satellite Infrastructure Subscription 清单。Satellite 必须启用并同步 satellite-capsule-6.x 存储库。要在客户门户网站中创建、管理和导出红帽订阅清单，请参阅在 *Subscription Central* 中为连接的 Satellite 服务器创建和管理清单。

Satellite 服务器和 Capsule 服务器不支持主机名中的短名称。使用自定义证书时，自定义证书的通用名称(CN)必须是完全限定域名(FQDN)，而不是短名称。这不适用于 Satellite 的客户端。

在安装 Satellite 服务器前，请确保您的环境满足安装要求。

必须在全新调配的系统上安装卫星服务器，该系统上不提供其他功能，但运行 Satellite 服务器除外。新置备的系统不能有外部身份提供程序提供的以下用户，以避免与 Satellite 服务器创建的本地用户冲突：

- Apache
- Foreman
- foreman-proxy
- postgres
- Pulp
- puppet
- redis
- tomcat

认证的虚拟机监控程序

在运行 Red Hat Enterprise Linux 的虚拟机监控程序上运行的物理系统和虚拟机上完全支持 Satellite 服务器。有关认证虚拟机监控程序的更多信息，请参阅 Red Hat OpenStack Platform、Red Hat Virtualization、Red Hat OpenShift Virtualization 和带有 KVM 的 Red Hat Enterprise Linux 中的认证的客户机操作系统。

SELinux 模式

SELinux 必须启用，可以是 enforcing 模式或 permissive 模式。不支持在禁用 SELinux 的情况下安装。

FIPS 模式

您可以在以 FIPS 模式运行的 Red Hat Enterprise Linux 系统上安装 Satellite。安装 Satellite 后您无法启用 FIPS 模式。如需更多信息，请参阅 *安全强化* 中的 安装启用了 FIPS 模式的 RHEL 8 系统 。

注意

Satellite 支持 DEFAULT 和 FIPS 加密策略。FUTURE 加密策略不支持 Satellite 和 Capsule 安装 。FUTURE 策略是一种更严格的前进安全级别，用于测试可能的未来策略。如需更多信息，请参阅 Red Hat Enterprise Linux 指南中的 使用系统范围的加密策略。

Satellite 间同步(ISS)

在 air-gapped Satellite 服务器的情况下，所有 Satellite 服务器都必须位于同一 Satellite 版本中，才能使 ISS 导出同步正常工作。ISS 网络同步可用于支持它的所有 Satellite 版本。如需更多信息，请参阅 *管理内容 中的 在 Satellite 服务器间同步 内容*。

1.2. 存储要求

下表详细介绍了特定目录的存储要求。这些值基于预期的用例场景，并根据各个环境的不同而有所不同。

运行时大小由 Red Hat Enterprise Linux 6、7 和 8 软件仓库同步来测量。

表 1.1. Satellite 服务器安装的存储要求

目录	安装大小	运行时大小
/var/log	10 MB	10 GB
/var/lib/pgsql	100 MB	20 GB
/usr	5 GB	不适用
/opt/puppetlabs	500 MB	不适用
/var/lib/pulp	1 MB	300 GB

对于外部数据库服务器： **/var/lib/pgsql**，安装大小为 100 MB，运行时大小为 20 GB。

有关分区和大小的详细信息，请参阅 *Red Hat Enterprise Linux 8 系统设计指南* 中的分区参考。

1.3. 存储指南

安装 Satellite 服务器以提高效率时，请考虑以下准则。

- 如果将 **/tmp** 目录挂载为单独的文件系统，则必须使用 **/etc/fstab** 文件中的 **exec** 挂载选项。如果 **/tmp** 已经挂载了 **noexec** 选项，您必须将选项更改为 **exec** 并重新挂载文件系统。这是 **puppetserver** 服务正常工作的要求。
- 由于大多数 Satellite 服务器数据存储在 **/var** 目录中，所以在 LVM 存储上挂载 **/var** 可帮助系统扩展。
- 对 **/var/lib/pulp/** 目录使用高带宽、低延迟存储。因为 Red Hat Satellite 有很多 I/O 密集型操作，使用高延迟，低带宽存储会导致性能下降。确保您的安装速度在每秒 60 – 80 MB。

您可以使用 **storage-benchmark** 脚本获取此数据。有关使用 **storage-benchmark** 脚本的更多信息，请参阅 对 Satellite 操作的影响。

文件系统指南

- 不要使用 GFS2 文件系统，因为输入输出延迟太高。

日志文件存储

日志文件被写入 **/var/log/messages/**、**/var/log/httpd/** 和 **/var/lib/foreman-proxy/openscap/content/**。您可以使用 **logrotate** 管理这些文件的大小。如需更多信息，请参阅 如何使用 logrotate 工具来轮转日志文件。

日志消息所需的存储量取决于您的安装和设置。

NFS 挂载的 SELinux 注意事项

当使用 NFS 共享挂载 **/var/lib/pulp** 目录时，SELinux 会阻止同步过程。要避免这种情况，请在文件系统表中指定 **/var/lib/pulp** 目录的 SELinux 上下文，方法是在 **/etc/fstab** 中添加以下行：

```
nfs.example.com:/nfsshare  /var/lib/pulp  nfs  context="system_u:object_r:var_lib_t:s0"  1 2
```

如果 NFS 共享已经挂载，请使用上述配置重新挂载它，并输入以下命令：

```
# restorecon -R /var/lib/pulp
```

重复的软件包

不同存储库中重复的软件包仅在磁盘上存储一次。包含重复软件包的其他软件仓库需要较少的额外存储。批量存储位于 **/var/lib/pulp/** 目录中。这些端点无法手动配置。确保 **/var** 文件系统上可用存储以防止存储问题。

符号链接

您不能对 **/var/lib/pulp/** 使用符号链接。

同步 RHEL ISO

如果您计划将 RHEL 内容 ISO 与 Satellite 同步，请注意，Red Hat Enterprise Linux 的所有次要版本也会同步。您必须计划在 Satellite 上有足够的存储来管理这一点。

1.4. 支持的操作系统

您可以使用磁盘、本地 ISO 镜像、Kickstart 或者红帽支持的任何其他方法安装操作系统。Red Hat Satellite Server 在最新版本的 Red Hat Enterprise Linux 8 上被支持，该版本可在 Satellite 服务器安装时可用。以前的 Red Hat Enterprise Linux 版本（包括 EUS 或 z-stream）不被支持。

以下操作系统由安装程序支持，有软件包，并经过测试以部署 Satellite：

表 1.2. satellite-installer 支持的操作系统

操作系统	架构	备注
Red Hat Enterprise Linux 8	仅限 x86_64	

红帽建议使用现有系统，因为 Satellite 安装程序会影响多个组件的配置。Red Hat Satellite Server 需要具有 **@Base** 软件包组的 Red Hat Enterprise Linux 安装，没有其他软件包集修改，而不需要第三方配置或软件直接进行服务器直接操作。这个限制包括强化和其他非红帽安全软件。如果您的基础架构中需要此类软件，请首先安装和验证完整的 Satellite 服务器，然后再添加任何非红帽软件。

红帽不支持对运行 Satellite 服务器以外的任何系统使用系统。

1.5. 支持的浏览器

Satellite 支持最新版本的 Firefox 和 Google Chrome 浏览器。

Satellite Web UI 和命令行界面支持英语、葡萄牙语、简体中文、韩语、日语、意大利语、西班牙语、俄语、法语和德语。

1.6. 端口和防火墙要求

要使 Satellite 架构的组件进行通信，请确保在基础操作系统上开放和释放所需的网络端口。您还必须确保在任何基于网络的防火墙上打开所需的网络端口。

使用这些信息来配置任何基于网络的防火墙。请注意，一些解决方案必须专门配置为允许机器之间的通信，因为它们与基于网络的防火墙类似。如果您使用基于应用程序的防火墙，请确保基于应用程序的防火墙允许表中列出的所有应用程序以及防火墙已知的应用程序。如果可能，禁用应用程序检查并允许基于协议打开的端口通信。

集成胶囊

Satellite 服务器具有集成胶囊，且直接连接到 Satellite 服务器的任何主机都是本节上下文中的 Satellite 客户端。这包括在其上运行胶囊式服务器的基本操作系统。

Capsule 的客户端

是胶囊（除 Satellite 集成胶囊之外的）的客户端不需要访问卫星服务器的主机。如需有关 Satellite 拓扑和端口连接图的更多信息，请参阅 *概述、概念和部署注意事项* 中的 Capsule Networking。

所需端口可能会根据您的配置而改变。

下表指定目的地端口和网络流量的方向：

表 1.3. Satellite 服务器传入流量

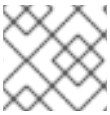
目的地端口	协议	服务	源	必需 For	描述

53	TCP 和 UDP	DNS	DNS 服务器和客户端	名称解析	DNS （可选）
67	UDP	DHCP	客户端	动态 IP	DHCP （可选）
69	UDP	TFTP	客户端	TFTP 服务器（可选）	
443	TCP	HTTPS	Capsule	Red Hat Satellite API	来自 Capsule 的通信
443, 80	TCP	HTTPS, HTTP	客户端	全局注册	将主机注册到 Satellite 注册启动、上传事实和发送已安装的软件包和追踪需要端口 443 端口 80 在注册完成的 **/unattended/built** 端点上通知 Satellite
443	TCP	HTTPS	Red Hat Satellite	内容镜像	管理
443	TCP	HTTPS	Red Hat Satellite	Capsule API	智能代理功能
443, 80	TCP	HTTPS, HTTP	Capsule	内容检索	内容
443, 80	TCP	HTTPS, HTTP	客户端	内容检索	内容
1883	TCP	MQTT	客户端	基于 REX 的拉取（可选）	REX 作业通知的内容主机（可选）
5910 – 5930	TCP	HTTPS	浏览器	计算资源的虚拟控制台	
8000	TCP	HTTP	客户端	置备模板	用于客户端安装程序、iPXE 或 UEFI HTTP 引导的模板检索
8000	TCP	HTTPS	客户端	PXE 引导	安装

8140	TCP	HTTPS	客户端	Puppet 代理	客户端更新（可选）
9090	TCP	HTTPS	Red Hat Satellite	Capsule API	智能代理功能
9090	TCP	HTTPS	客户端	OpenSCAP	配置客户端（如果安装了 OpenSCAP 插件）
9090	TCP	HTTPS	发现的节点	Discovery（发现）	主机发现和置备（如果安装了发现插件）

任何直接连接到 Satellite 服务器的主机都是此上下文中的客户端，因为它是集成胶囊的客户端。这包括在其上运行胶囊式服务器的基本操作系统。

DHCP Capsule 将执行 ICMP ping 或 TCP echo 连接尝试子网中 DHCP IPAM 设置的主机，以找出被视为使用的 IP 地址是空闲的。可以使用 **satellite-installer --foreman-proxy-dhcp-ping-free-ip=false** 关闭此行为。



注意

有些传出流量返回到 Satellite，以启用内部通信和安全操作。

表 1.4. Satellite 服务器传出流量

目的地端口	协议	服务	目的地	必需 For	描述
	ICMP	ping	客户端	DHCP	空闲 IP 检查（可选）
7	TCP	echo	客户端	DHCP	空闲 IP 检查（可选）
22	TCP	SSH	目标主机	远程执行	运行作业
22, 16514	TCP	SSH/TLS	计算资源	Satellite 源自通信，用于 libvirt 中的计算资源	
53	TCP 和 UDP	DNS	互联网上的 DNS 服务器	DNS 服务器	解析 DNS 记录（可选）
53	TCP 和 UDP	DNS	DNS 服务器	胶囊 DNS	验证 DNS 冲突（可选）
53	TCP 和 UDP	DNS	DNS 服务器	编配	验证 DNS 冲突

目的地端口	协议	服务	目的地	必需 For	描述
68	UDP	DHCP	客户端	动态 IP	DHCP （可选）
80	TCP	HTTP	远程存储库	内容同步	远程仓库
389, 636	TCP	LDAP, LDAPS	外部 LDAP 服务器	LDAP	LDAP 身份验证，只有在启用了外部身份验证时才需要。定义 **LDAPAuthSource** 时可以自定义端口
443	TCP	HTTPS	Satellite	Capsule	Capsule 配置管理 模板检索 OpenSCAP 远程执行结果上传
443	TCP	HTTPS	Amazon EC2, Azure, Google GCE	计算资源	虚拟机交互 (query/create/destroy) （可选）
443	TCP	HTTPS	console.redhat.com	Red Hat Cloud plugin API 调用	
443	TCP	HTTPS	cdn.redhat.com	内容同步	Red Hat CDN
443	TCP	HTTPS	api.access.redhat.com	SOS 报告	通过红帽客户门户网站 提供支持问题单（可选）
443	TCP	HTTPS	cert-api.access.redhat.com	遥测数据上传和报告	
443	TCP	HTTPS	Capsule	内容镜像	启动
443	TCP	HTTPS	Infoblox DHCP Server	DHCP 管理	当使用 Infoblox 进行 DHCP 时，管理 DHCP 租期（可选）

目的地端口	协议	服务	目的地	必需 For	描述
623			客户端	电源管理	BMC On/Off/Cycle/Status
5000	TCP	HTTPS	OpenStack 计算资源	计算资源	虚拟机交互 (query/create/destroy) （可选）
5900 – 5930	TCP	SSL/TLS	虚拟机监控程序	noVNC 控制台	启动 noVNC 控制台
7911	TCP	DHCP、OMAPI	DHCP Server	DHCP	DHCP 目标使用 **--foreman-proxy-dhcp-server** 配置，默认为 localhost ISC 和 **remote_isc** 使用默认为 7911 的可配置端口，并使用 OMAPI
8443	TCP	HTTPS	客户端	Discovery（发现）	Capsule 将 reboot 命令发送到发现的主机（可选）
9090	TCP	HTTPS	Capsule	Capsule API	管理 Capsule

1.7. 启用从客户端到 SATELLITE 服务器的连接

属于 Satellite 服务器内部胶囊的客户端的胶囊和内容主机需要通过 Satellite 的基于主机的防火墙和任何基于网络的防火墙访问。

使用这个流程在安装 Satellite 的系统上配置基于主机的防火墙，从客户端启用进入连接，并在系统重启后保留配置。有关使用 的端口 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 端口和防火墙要求*。

流程

1. 在 Satellite 服务器上为客户端打开端口：

```
# firewall-cmd \
--add-port="5647/tcp" \
--add-port="8000/tcp" \
--add-port="9090/tcp"
```

2. 允许访问 Satellite 服务器上的服务：

```
# firewall-cmd \
--add-service=dns \
--add-service=dhcp \
--add-service=tftp \
--add-service=http \
--add-service=https \
--add-service=puppetmaster
```

3. 使更改持久：

```
# firewall-cmd --runtime-to-permanent
```

验证

- 输入以下命令：

```
# firewall-cmd --list-all
```

如需更多信息，请参阅 *Red Hat Enterprise Linux 8 保护网络* 中的 使用和配置 firewalld。

1.8. 验证 DNS 解析

使用完全限定域名验证完整正向和反向 DNS 解析，以防止安装 Satellite 时出现问题。

流程

1. 确保主机名和本地主机正确解析：

```
# ping -c1 localhost
# ping -c1 `hostname -f` # my_system.domain.com
```

成功名称解析结果结果类似如下：

```
# ping -c1 localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.043 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.043/0.043/0.043/0.000 ms

# ping -c1 `hostname -f`
PING hostname.gateway (XX.XX.XX.XX) 56(84) bytes of data.
64 bytes from hostname.gateway (XX.XX.XX.XX): icmp_seq=1 ttl=64 time=0.019 ms

--- localhost.gateway ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.019/0.019/0.019/0.000 ms
```

2. 要避免使用静态和临时主机名的差异，请输入以下命令设置系统中的所有主机名：

```
# hostnamectl set-hostname name
```

如需更多信息，请参阅 *Red Hat Enterprise Linux 8 配置和管理网络* 中的 使用 hostnamectl 更改主机名。

警告

名称解析对于 Satellite 的操作至关重要。如果 Satellite 无法正确解析其完全限定域名，则内容管理、订阅管理和置备等任务将失败。

1.9. 使用预定义的配置集调整 SATELLITE 服务器

如果您的 Satellite 部署包含超过 5000 个主机，您可以使用预定义的调优配置文件来提高 Satellite 的性能。

请注意，您不能在 Capsules 上使用调优配置集。

您可以根据 Satellite 管理的主机数量和可用的硬件资源选择其中一个配置集。

调优配置文件位于 **/usr/share/foreman-installer/config/foreman.hiera/tuning/sizes** 目录中。

当您使用 **--tuning** 选项运行 **satellite-installer** 命令时，部署配置设置将按照以下顺序应用到 Satellite：

1. **/usr/share/foreman-installer/config/foreman.hiera/tuning/common.yaml** 文件中定义的默认调优配置文件
2. 要应用到部署的调优配置文件，并在 **/usr/share/foreman-installer/config/foreman.hiera/tuning/sizes/** 目录中定义
3. 可选：如果您配置了 **/etc/foreman-installer/custom-hiera.yaml** 文件，Satellite 会应用这些配置设置。

请注意，**/etc/foreman-installer/custom-hiera.yaml** 文件中定义的配置设置会覆盖在调优配置文件中定义的配置设置。

因此，在应用调优配置文件前，您必须比较 **/usr/share/foreman-installer/config/foreman.hiera/tuning/common.yaml** 中默认调优配置文件中定义的配置设置，并从 **/etc/foreman- installer/custom-hiera.yaml** 文件中删除任何重复的配置。

default

主机数量：0wagon-wagon5000
RAM: 20G

CPU 内核数：4

中

主机数量：5001 iwl-wagon10000
RAM: 32G

CPU 内核数：8

大

主机数量： 10001wagon-wagon20000
RAM: 64G

CPU 内核数：16

extra-large

主机数量： 20001.4-1.-wagon60000
RAM：128G

CPU 内核数：32

extra-extra-large

主机数量：60000+
RAM: 256G

CPU 内核数： 48+

流程

1. 可选： 如果您在 Satellite 服务器上配置了 **custom-hiera.yaml** 文件，请将 **/etc/foreman-installer/custom-hiera.yaml** 文件备份到 **custom-hiera.original**。如果文件损坏，您可以使用备份文件将 **/etc/foreman-installer/custom-hiera.yaml** 文件恢复到其原始状态：

```
# cp /etc/foreman-installer/custom-hiera.yaml \
/etc/foreman-installer/custom-hiera.original
```

2. 可选： 如果您在 Satellite 服务器上配置了 **custom-hiera.yaml** 文件，请查看 **/usr/share/foreman-installer/config/foreman.hiera/tuning/common.yaml** 中默认调优配置文件的定义，以及您要应用到 **/usr/share/foreman-installer/config/foreman.hiera/tuning/sizes/** 中的。将配置条目与您的 **/etc/foreman-installer/custom-hiera.yaml** 文件中的条目进行比较，并删除 **/etc/foreman-installer/custom-hiera.yaml** 文件中的任何重复配置设置。

3. 使用您要应用的配置文件的 **--tuning** 选项输入 **satellite-installer** 命令。例如，要应用中型调优配置文件设置，请输入以下命令：

```
# satellite-installer --tuning medium
```

第 2 章 在 IPV6 网络中为 SATELLITE 安装准备您的环境

您可以在 IPv6 网络中安装和使用 Satellite。在 IPv6 网络中安装 Satellite 前，请查看限制并确保您满足这些要求。

要在 IPv6 网络中置备主机，在安装 Satellite 后，还必须为 UEFI HTTP 引导置备配置 Satellite。如需更多信息，请参阅 第 4.5 节 “在 IPv6 网络中为 UEFI HTTP 引导置备配置 Satellite” 。

2.1. IPV6 网络中 SATELLITE 安装的限制

IPv6 网络中安装 Satellite 有以下限制：

- 您可以在 IPv6 系统上安装 Satellite 和 Capsule，不支持双栈安装。
- 虽然 Satellite 置备模板包括对 PXE 和 HTTP (iPXE)配置的 IPv6 支持，但唯一经过测试和验证的调配工作流是 UEFI HTTP 引导调配。这个限制仅与计划使用 Satellite 置备主机的用户相关。

2.2. 在 IPV6 网络中安装 SATELLITE 的要求

在 IPv6 网络中安装 Satellite 前，请确定您满足以下要求：

- 您必须将外部 DHCP IPv6 服务器部署为单独的非受管服务，将客户端引导至 GRUB2 中，然后使用 DHCPv6 配置 IPv6 网络或分配静态 IPv6 地址。这是必要的，因为 Red Hat Enterprise Linux (ISC DHCP)中的 DHCP 服务器不提供管理 IPv6 记录的集成 API，因此提供 DHCP 管理的 Capsule DHCP 插件仅限于 IPv4 子网。
- 您必须部署支持 IPv4 和 IPv6 的外部 HTTP 代理服务器。这是必要的，因为 Red Hat Content Delivery Network 只通过 IPv4 网络发布内容，因此您必须使用此代理将内容拉取到 IPv6 网络上的 Satellite 中。
- 您必须将 Satellite 配置为使用此双堆栈（支持 IPv4 和 IPv6）HTTP 代理服务器作为默认代理。如需更多信息，请参阅 向 Satellite 添加默认 HTTP 代理 。

第 3 章 安装 SATELLITE 服务器

从连接的网络安装 Satellite 服务器时，您可以获取软件包并直接从 Red Hat Content Delivery Network 接收更新。

注意

您不能将 Satellite 服务器注册到自己。

使用以下步骤安装 Satellite 服务器、执行初始配置和导入订阅清单。有关订阅清单的更多信息， *请参阅管理内容中的红帽订阅*。

请注意，Satellite 安装脚本基于 Puppet，这意味着如果您多次运行安装脚本，则可能会覆盖任何手动配置更改。为了避免这种情况，并确定将来的更改适用，请在运行安装脚本时使用 **--noop** 参数。此参数可确保不进行实际更改。潜在的更改被写入 **/var/log/foreman-installer/satellite.log**。

文件始终被备份，以便您可以恢复任何不需要的更改。例如，在 foreman-installer 日志中，您可以看到一个类似于 Filebucket 的条目：

```
/Stage[main]/Dhcp/File[/etc/dhcp/dhcpd.conf]: Filebucketed /etc/dhcp/dhcpd.conf to puppet with sum
622d9820b8e764ab124367c68f5fa3a1
```

您可以恢复以前的文件，如下所示：

```
# puppet filebucket -l \
restore /etc/dhcp/dhcpd.conf 622d9820b8e764ab124367c68f5fa3a1
```

3.1. 配置 HTTP 代理以连接到 RED HAT CDN

先决条件

您的网络网关和 HTTP 代理必须允许访问以下主机：

主机名	端口	协议
subscription.rhsm.redhat.com	443	HTTPS
cdn.redhat.com	443	HTTPS
*.akamaiedge.net	443	HTTPS
cert.console.redhat.com （如果使用 Red Hat Insights）	443	HTTPS
api.access.redhat.com （如果使用 Red Hat Insights）	443	HTTPS
cert-api.access.redhat.com （如果使用 Red Hat Insights）	443	HTTPS

Satellite 服务器使用 SSL 来安全地与红帽 CDN 通信。SSL 拦截器代理会干扰这个通信。这些主机必须在 HTTP 代理上允许列表。

有关红帽 CDN (cdn.redhat.com)使用的 IP 地址列表，请参阅红帽客户门户网站上 红帽的公共 CIDR 列表。

要使用 HTTP 代理配置订阅管理器，请按照以下步骤操作。

流程

1. 在 Satellite 服务器上，在 **/etc/rhsm/rhsm.conf** 文件中完成以下详情：

```
# an http proxy server to use (enter server FQDN)
proxy_hostname = myproxy.example.com

# port for http proxy server
proxy_port = 8080

# user name for authenticating to an http proxy, if needed
proxy_user =

# password for basic http proxy auth, if needed
proxy_password =
```

3.2. 注册到 RED HAT SUBSCRIPTION MANAGEMENT

将主机注册到红帽订阅管理可让主机订阅和使用用户所有可用订阅的内容。这包括 Red Hat Enterprise Linux 和 Red Hat Satellite 等内容。

流程

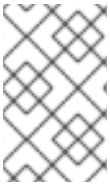
- 使用 Red Hat Content Delivery Network 注册您的系统，在提示时输入您的客户门户网站用户名和密码：

```
# subscription-manager register
```

该命令显示类似如下的输出：

```
# subscription-manager register
Username: user_name
Password:
The system has been registered with ID: 541084ff2-44cab-4eb1-9fa1-7683431bcf9a
```

3.3. 附加 SATELLITE 基础架构订阅



注意

如果您在红帽客户门户网站上启用了 SCA，请跳过这一步。不需要使用 subscription-manager 将 Red Hat Satellite Infrastructure 订阅附加到 Satellite Server。有关 SCA 的更多信息，请参阅简单内容访问。

注册了 Satellite 服务器后，您必须识别您的订阅池 ID 并附加一个可用订阅。Red Hat Satellite Infrastructure 订阅提供对 Red Hat Satellite 和 Red Hat Enterprise Linux 内容的访问。

Red Hat Satellite Infrastructure 包括在所有包括 Satellite 的订阅中，以前称为 智能管理。如需更多信息，请参阅*红帽知识库*中的 Satellite 基础架构订阅 MCT3718 MCT3719。

如果订阅尚未附加到系统，则订阅被归类为可用。如果您无法找到可用的 Satellite 订阅，请查看红帽知识库解决方案 如何找出在 Red Hat Subscription Manager 下注册的客户端使用了哪个订阅？ 运行脚本以查看另一个系统是否消耗了您的订阅。

流程

1. 确定 Satellite 基础架构订阅的池 ID：

```
# subscription-manager list --all --available --matches 'Red Hat Satellite Infrastructure Subscription'
```

该命令显示类似如下的输出：

```
Subscription Name:   Red Hat Satellite Infrastructure Subscription
Provides:            Red Hat Satellite
                     Red Hat Software Collections (for RHEL Server)
                     Red Hat CodeReady Linux Builder for x86_64
                     Red Hat Satellite Capsule
                     Red Hat Ansible Engine
                     Red Hat Satellite with Embedded Oracle
                     Red Hat Satellite 5 Managed DB
                     Red Hat Enterprise Linux Load Balancer (for RHEL Server)
                     Red Hat Beta
                     Red Hat Software Collections Beta (for RHEL Server)
                     Red Hat Enterprise Linux Server
                     Red Hat Enterprise Linux for x86_64
                     Red Hat Satellite Proxy
                     Red Hat Enterprise Linux High Availability for x86_64
                     Red Hat Discovery
SKU:                 MCT3718
Contract:
Pool ID:             8aca43dd771bf31101771c0231f906a5
Provides Management: Yes
Available:           10
Suggested:           1
Service Type:        L1-L3
Roles:
Service Level:       Premium
Usage:
Add-ons:
Subscription Type:   Standard
Starts:              11/11/2020
Ends:                11/11/2023
Entitlement Type:    Physical
```

2. 记录订阅池 ID。您的订阅池 ID 与提供的示例不同。

3. 将 Satellite 基础架构订阅连接到您的 Satellite Server 在其上运行的基本操作系统中。如果 Satellite 服务器上启用了 SCA，您可以跳过此步骤：

-

```
# subscription-manager attach --pool=pool_id
```

该命令显示类似如下的输出：

```
Successfully attached a subscription for: Red Hat Satellite Infrastructure Subscription
```

4. 可选：验证是否已附加 Satellite Infrastructure 订阅：

```
# subscription-manager list --consumed
```

3.4. 配置软件仓库

使用以下步骤启用安装 Satellite 服务器所需的存储库。

1. 禁用所有软件仓库：

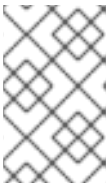
```
# subscription-manager repos --disable "*"
```

2. 启用以下软件仓库：

```
# subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms \
--enable=rhel-8-for-x86_64-appstream-rpms \
--enable=satellite-6.15-for-rhel-8-x86_64-rpms \
--enable=satellite-maintenance-6.15-for-rhel-8-x86_64-rpms
```

3. 启用 DNF 模块：

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



注意

如果在启用 **satellite:el8** 模块时有任何与 Ruby 或 PostgreSQL 冲突的警告，请参阅 *附录 A, DNF 模块故障排除*。有关 Red Hat Enterprise Linux 8 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 。

3.5. 可选：在 SATELLITE 服务器上使用 FAPOLICYD

通过在 Satellite 服务器上启用 **fapolicyd**，您可以通过监控和控制对文件和目录的访问来提供额外的安全层。fapolicyd 守护进程使用 RPM 数据库作为可信二进制文件和脚本的存储库。

您可以在 Satellite 服务器或 Capsule 服务器上打开或关闭 fapolicyd。

3.5.1. 在 Satellite 服务器上安装 fapolicyd

您可以与 Satellite 服务器一起安装 **fapolicyd**，也可以安装到现有的 Satellite 服务器上。如果您要安装 **fapolicyd** 和新的 Satellite 服务器，安装过程会在 Red Hat Enterprise Linux 主机中检测到 fapolicyd，并自动部署 Satellite 服务器规则。

先决条件

- 确保您的主机可以访问 Red Hat Enterprise Linux 的 BaseOS 软件仓库。

流程

1. 安装 fapolicyd ：

```
# dnf install fapolicyd
```

2. 启动 **fapolicyd** 服务：

```
# systemctl enable --now fapolicyd
```

验证

- 验证 **fapolicyd** 服务是否正常运行：

```
# systemctl status fapolicyd
```

新的 Satellite 服务器或 Capsule 服务器安装

如果新的 Satellite 服务器或 Capsule 服务器安装，请在 Red Hat Enterprise Linux 主机上安装并启用 fapolicyd 后按照标准安装过程进行操作。

其他资源

有关 fapolicyd 的更多信息，请参阅 *Red Hat Enterprise Linux 8 安全强化* 中的 使用 fapolicyd 阻止和允许应用程序。

3.6. 安装 SATELLITE 服务器软件包

流程

1. 更新所有软件包：

```
# dnf update
```

2. 安装 Satellite 服务器软件包：

```
# dnf install satellite
```

3.7. 使用 CHRONYD 同步系统时钟

为最大程度降低时间偏移的影响，您必须将系统时钟与您要使用网络时间协议(NTP)服务器安装 Satellite 服务器的基本操作系统同步。如果基本操作系统时钟配置不正确，证书验证可能会失败。

有关 **chrony** 套件的更多信息，请参阅 *Red Hat Enterprise Linux 8 配置基本系统设置* 中的 使用 Chrony 套件配置 NTP。

流程

1. 安装 **chrony** 软件包：

```
# dnf install chrony
```

2. 启动并启用 **chronyd** 服务：

```
# systemctl enable --now chronyd
```

3.8. 在基本操作系统中安装 SOS 软件包

在基础操作系统上安装 **sos** 软件包，以便您可以从 Red Hat Enterprise Linux 系统中收集配置和诊断信息。您还可以使用它提供初始系统分析，在打开红帽技术支持的服务请求时需要这样做。有关使用 **sos** 的更多信息，请参阅 知识库解决方案 什么是 sosreport 以及如何在 Red Hat Enterprise Linux 4.6 及之后的版本中创建？

流程

- 安装 **sos** 软件包：

```
# satellite-maintain packages install sos
```

3.9. 配置 SATELLITE 服务器

使用 **satellite-installer** 安装脚本安装 Satellite 服务器。

这个方法是通过一个或多个命令选项运行安装脚本来执行。命令选项覆盖对应的默认初始配置选项，并记录在 Satellite 回答文件中。您可以根据需要运行脚本来配置任何必要的选项。

3.9.1. 配置 Satellite 安装

此初始配置流程创建机构、位置、用户名和密码。在初始配置后，如果需要，您可以创建额外的机构和位置。初始配置还会在同一服务器上安装 PostgreSQL 数据库。

安装过程可能需要十分钟才能完成。如果您要远程连接到系统，请使用允许挂起和重新附加通信会话的工具，以便在从远程系统断开连接时检查安装过程。**如果您丢失了与运行安装命令的 shell 的连接，请参阅 /var/log/foreman-installer/satellite.log 的日志，以确定进程是否已成功完成。**

注意事项

- **使用 satellite-installer --scenario satellite --help 命令显示可用选项和任何默认值。如果没有指定任何值，则使用默认值。**

- 为 选项**指定一个有意义的值： --foreman-initial-organization。这可以是您的公司名称。也会创建与值匹配的内部标签，之后无法更改。如果没有指定值，则会创建一个名为 Default Organization 的组织，其标签为 Default_Organization。您可以重命名机构名称，但不能重命名标签。**

- **默认情况下，由安装程序配置的所有配置文件都被管理。当 satellite-installer 运行时，它会使用预期值覆盖对受管文件的任何手动更改。这意味着，在损坏的系统上运行安装程序应该将其**

恢复到工作顺序，无论进行了什么更改。有关如何对其他服务应用自定义配置的更多信息，请参阅将自定义 配置应用到 Satellite。

流程

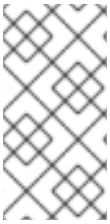
1. 输入以下命令以及您要使用的任何附加选项：

```
# satellite-installer --scenario satellite \
--foreman-initial-organization "My_Organization" \
--foreman-initial-location "My_Location" \
--foreman-initial-admin-username admin_user_name \
--foreman-initial-admin-password admin_password
```

脚本显示其进度，并将日志写入 /var/log/foreman-installer/satellite.log。

3.10. 将红帽订阅清单导入到 SATELLITE 服务器中

使用以下步骤将红帽订阅清单导入到 Satellite 服务器中。



注意

在机构上设置简单内容访问(SCA)，而不是清单。导入清单不会更改您机构的简单内容访问状态。

先决条件

- 您必须有一个 从红帽客户门户网站导出的红帽订阅 清单文件。如需更多信息，请参阅 *使用红帽订阅管理 中的创建和管理 清单*。

流程

1. 在 Satellite Web UI 中，确保将上下文设置为您要使用的组织。
2. 在 Satellite Web UI 中，进入到 Content > Subscriptions 并点 Manage Manifest。
3. 在 Manage Manifest 窗口中，单击 Choose File。

4. 导航到包含红帽订阅清单文件的位置，然后单击 **Open**。

CLI 过程

1. 将红帽订阅清单文件从本地机器复制到 Satellite 服务器：

```
$ scp ~/manifest_file.zip root@satellite.example.com:~/.
```

2. 以 root 用户身份登录 Satellite 服务器，再导入 Red Hat 订阅清单文件：

```
# hammer subscription upload \
--file ~/manifest_file.zip \
--organization "My_Organization"
```

现在，您可以启用软件仓库并导入红帽内容。如需更多信息，*请参阅管理内容中的导入内容*。

第 4 章 在 SATELLITE 服务器上执行其他配置

4.1. 将 RED HAT INSIGHTS 与 SATELLITE 服务器搭配使用

您可以使用 Red Hat Insights 诊断与安全漏洞相关的系统和停机时间，性能降级和稳定性故障。您可以使用控制面板快速识别稳定性、安全性和性能的关键风险。您可以根据类别排序，查看影响和解决方案的详情，然后确定受影响的系统。

请注意，您不需要订阅清单中的 Red Hat Insights 权利。有关 Satellite 和 Red Hat Insights 的更多信息，请参阅 Red Hat Insights on Satellite Red Hat Enterprise Linux (RHEL)。

要维护您的 Satellite 服务器，并改进您的功能来监控和诊断您使用 Satellite 的问题，请在 Satellite 服务器上安装 Red Hat Insights，并使用 Red Hat Insights 注册 Satellite 服务器。

调度 insights-client

请注意，您可以通过在 Satellite 上配置 insights-client.timer 来更改运行 insights-client 的默认调度。如需更多信息，*请参阅 Red Hat Insights 的客户端配置指南* 中的 更改 insights-client 调度。

流程

1. 要在 Satellite 服务器上安装 Red Hat Insights，请输入以下命令：

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

2. 要将 Satellite 服务器注册到 Red Hat Insights，请输入以下命令：

```
# satellite-installer --register-with-insights
```

4.2. 禁用 RED HAT INSIGHTS 注册

安装或升级 Satellite 后，您可以根据需要选择取消注册或注册 Red Hat Insights。例如，如果您需要在断开连接的环境中使用 Satellite，您可以从 Satellite 服务器取消注册 insights-client。

先决条件

1. 您已在红帽客户门户网站中注册了 Satellite。

流程

1. 可选：要从 Satellite 服务器取消注册 Red Hat Insights，请输入以下命令：

```
# insights-client --unregister
```

2. 可选：要在 Red Hat Insights 中注册 Satellite 服务器，请输入以下命令：

```
# satellite-installer --register-with-insights
```

4.3. 启用和同步 SATELLITE 客户端 6 存储库

Satellite Client 6 存储库为注册到 Satellite 的主机提供 katello-host-tools 和 puppet 软件包。您必须定期将软件仓库从 Red Hat Content Delivery Network (CDN)同步到 Satellite 服务器，并在主机上启用存储库。

4.3.1. 为 Red Hat Enterprise Linux 9 和 Red Hat Enterprise Linux 8 同步 Satellite Client 6 软件仓库

要使用 CLI 而不是 Satellite Web UI，请查看与 Red Hat Enterprise Linux 版本相关的流程：

- Red Hat Enterprise Linux 9 的 CLI 步骤
- Red Hat Enterprise Linux 8 的 CLI 步骤

流程

1. 在 Satellite Web UI 中，进入到 Content > Sync Status。
2. 单击 Red Hat Enterprise Linux for x86_64 产品旁边的箭头，以查看可用的内容。
3. 选择 Red Hat Satellite Client 6 for RHEL 9 x86_64 RPMs 或 Red Hat Satellite Client 6 for RHEL 8 x86_64 RPMs。
4. 点 Synchronize Now。

Red Hat Enterprise Linux 9 的 CLI 步骤

- **同步 Satellite 客户端 6 存储库：**

```
# hammer repository synchronize \
--name "Red Hat Satellite Client 6 for RHEL 9 x86_64 RPMs" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux for x86_64"
```

Red Hat Enterprise Linux 8 的 CLI 步骤

- **同步 Satellite 客户端 6 存储库：**

```
# hammer repository synchronize \
--name "Red Hat Satellite Client 6 for RHEL 8 x86_64 RPMs" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux for x86_64"
```

其他资源

- **有关 hammer 存储库 synchronize 命令的详情，请输入 hammer 存储库 synchronize --help。**

4.3.2. 为 Red Hat Enterprise Linux 7 和 Red Hat Enterprise Linux 6 同步 Satellite Client 6 软件仓库

注意

您需要 Red Hat Enterprise Linux 延长生命周期支持(ELS)附加服务 来同步 Red Hat Enterprise Linux 6 的软件仓库。如需更多信息，请参阅 Red Hat Enterprise Linux Extended Lifecycle Support (ELS)附加服务 指南。

要使用 CLI 而不是 Satellite Web UI，请查看与 Red Hat Enterprise Linux 版本相关的流程：

- **Red Hat Enterprise Linux 7 的 CLI 步骤**
- **Red Hat Enterprise Linux 6 的 CLI 步骤**

流程

1. 在 Satellite Web UI 中，进入到 Content > Sync Status。

2. 单击 Red Hat Enterprise Linux Server 或 Red Hat Enterprise Linux Server - Extended Lifecycle Support 旁的箭头。

3. 根据您的操作系统版本，选择 Red Hat Satellite Client 6 (RHEL 7 Server) RPMs x86_64 或 Red Hat Satellite Client 6 for RHEL 6 Server - ELS RPMs x86_64。

4. 点 Synchronize Now。

Red Hat Enterprise Linux 7 的 CLI 步骤

- 同步 Satellite 客户端 6 存储库：

```
# hammer repository synchronize \
--async \
--name "Red Hat Satellite Client 6 for RHEL 7 Server RPMs x86_64" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux Server"
```

Red Hat Enterprise Linux 6 的 CLI 步骤

- 同步 Satellite 客户端 6 存储库：

```
# hammer repository synchronize \
--async \
--name "Red Hat Satellite Client 6 for RHEL 6 Server - ELS RPMs x86_64" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux Server - Extended Lifecycle Support"
```

其他资源

- 有关 hammer 存储库 synchronize 命令的详情，请输入 hammer 存储库 synchronize --help。

4.3.3. 为 Red Hat Enterprise Linux 9 和 Red Hat Enterprise Linux 8 启用 Satellite Client 6 软件仓库

要使用 CLI 而不是 Satellite Web UI，请查看与 Red Hat Enterprise Linux 版本相关的流程：

- Red Hat Enterprise Linux 9 的 CLI 步骤
- Red Hat Enterprise Linux 8 的 CLI 步骤

流程

1. 在 Satellite Web UI 中，进入到 Content > Red Hat Repositories。
2. 在 Available Repositories 窗格中，启用 recommended Repositories 来获取存储库列表。
3. 点 Red Hat Satellite Client 6 for RHEL 9 x86_64 (RPMs) 或 Red Hat Satellite Client 6 for RHEL 8 x86_64 (RPMs) 来扩展存储库集。
4. 对于 x86_64 架构，请单击 + 图标以启用该存储库。

如果 Satellite Client 6 项不可见，这可能是因为它们没有包含在从客户门户网站获取的红帽订阅清单中。要更正这一点，请登录到客户门户网站，添加这些软件仓库，下载红帽订阅清单并将其导入到 Satellite。如需更多信息，*请参阅管理内容中的管理红帽订阅*。

为每个主机上运行的 Red Hat Enterprise Linux 主版本启用 Satellite Client 6 软件仓库。启用红帽软件仓库后，会自动创建此软件仓库的产品。

Red Hat Enterprise Linux 9 的 CLI 步骤

- 启用 Satellite Client 6 存储库：

```
# hammer repository-set enable \
--basearch="x86_64" \
--name "Red Hat Satellite Client 6 for RHEL 9 x86_64 (RPMs)" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux for x86_64"
```

Red Hat Enterprise Linux 8 的 CLI 步骤

- 启用 Satellite Client 6 存储库：

```
# hammer repository-set enable \
--basearch="x86_64" \
--name "Red Hat Satellite Client 6 for RHEL 8 x86_64 (RPMs)" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux for x86_64"
```

其他资源

- 有关 **hammer repository-set enable** 命令的详情，请输入 **hammer repository-set enable --help**。

4.3.4. 为 Red Hat Enterprise Linux 7 和 Red Hat Enterprise Linux 6 启用 Satellite Client 6 软件仓库

注意

您需要 **Red Hat Enterprise Linux 延长生命周期支持(ELS)附加服务 才能启用 Red Hat Enterprise Linux 6 的软件仓库。如需更多信息，请参阅 Red Hat Enterprise Linux Extended Lifecycle Support (ELS)附加服务 指南。**

要使用 CLI 而不是 Satellite Web UI，请查看与 Red Hat Enterprise Linux 版本相关的流程：

- **Red Hat Enterprise Linux 7 的 CLI 步骤**
- **Red Hat Enterprise Linux 6 的 CLI 步骤**

流程

1. **在 Satellite Web UI 中，进入到 Content > Red Hat Repositories。**
2. **在 Available Repositories 窗格中，启用 recommended Repositories 来获取存储库列表。**
3. **在 Available Repositories 窗格中，点 Satellite Client 6 (for RHEL 7 Server) (RPMs) 或 Satellite Client 6 (for RHEL 6 Server - ELS) (RPMs) 来扩展存储库集。**

如果 Satellite Client 6 项不可见，这可能是因为它们没有包含在从客户门户网站获取的红帽订阅清单中。要更正这一点，请登录到客户门户网站，添加这些软件仓库，下载红帽订阅清单并

将其导入到 Satellite。如需更多信息，*请参阅管理内容中的管理红帽订阅*。

4. 对于 x86_64 架构，请单击 + 图标以启用该存储库。为每个主机上运行的 Red Hat Enterprise Linux 主版本启用 Satellite Client 6 软件仓库。启用红帽软件仓库后，会自动创建此软件仓库的产品。

Red Hat Enterprise Linux 7 的 CLI 步骤

- 启用 Satellite Client 6 存储库：

```
# hammer repository-set enable \
--basearch="x86_64" \
--name "Red Hat Satellite Client 6 (for RHEL 7 Server) (RPMs)" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux Server"
```

Red Hat Enterprise Linux 6 的 CLI 步骤

- 启用 Satellite Client 6 存储库：

```
# hammer repository-set enable \
--basearch="x86_64" \
--name "Red Hat Satellite Client 6 (for RHEL 6 Server - ELS) (RPMs)" \
--organization "My_Organization" \
--product "Red Hat Enterprise Linux Server - Extended Lifecycle Support"
```

其他资源

- 有关 hammer repository-set enable 命令的详情，请输入 hammer repository-set enable --help。

4.4. 在 SATELLITE 服务器上为拉取客户端配置远程执行

默认情况下，远程执行使用 SSH 作为 Script 供应商的传输机制。但是，远程执行还提供基于拉取的传输，如果您的基础架构禁止从 Satellite 到主机的传出连接，则可以使用它。

这包括 Satellite 上的 pull-mqtt 模式，以及主机上运行的拉取客户端。

注意

pull-mqtt 模式仅适用于 Script 提供程序。Ansible 和其他提供程序将继续使用其默认传输设置。

要在 Satellite 服务器上使用 pull-mqtt 模式，请按照以下步骤操作：

流程

1. 在 Satellite 服务器上启用基于拉取的传输：

```
# satellite-installer --foreman-proxy-plugin-remote-execution-script-mode pull-mqtt
```

2. 配置防火墙以允许端口 1883 上的 MQTT 服务：

```
# firewall-cmd --add-service=mqtt
```

在 pull-mqtt 模式中，主机向 Satellite 服务器或他们注册的任何胶囊服务器订阅作业通知。因此，建议确保 Satellite 服务器将远程执行作业发送到同一 Satellite 服务器或 Capsule 服务器。

3. 使更改持久：

```
# firewall-cmd --runtime-to-permanent
```

4. 在 Satellite Web UI 中，进入到 Administer > Settings。

5. 在 Content 选项卡上，将 Prefer registered through Capsule for remote execution 的值设为 Yes 。

在 Satellite 上设置基于拉取的传输后，您还必须在每个主机上进行配置。如需更多信息，*请参阅管理主机* 中的 远程执行的传输模式。

4.5. 在 IPV6 网络中为 UEFI HTTP 引导置备配置 SATELLITE

使用这个流程配置 Satellite，以使用 UEFI HTTP 引导置备 IPv6 网络中置备主机。

先决条件

- 确保您的客户端可以访问 DHCP 和 HTTP 服务器。
- 确保客户端可以访问 UDP 端口 67 和 68，以便客户端能够发送 DHCP 请求并接收 DHCP 提供。
- 确保为客户端打开 TCP 端口 8000，以便从 Satellite 和 Capsule 下载文件和 Kickstart 模板。
- 确保主机调配接口子网设置了 HTTP 引导胶囊，并且已设置了模板胶囊。有关更多信息，请参阅 *置备主机 中的 向 Satellite 服务器添加 子网*。
- 在 Satellite Web UI 中，导航到 Administer > Settings > Provisioning，并确保 Token duration 设置没有设为 0。由于未管理 DHCPv6 服务，Satellite 无法识别通过远程 IPv6 地址从网络引导的客户端，因此必须启用调配令牌。

流程

1. 您必须在安装程序中禁用 DHCP 管理，或者不使用它。
2. 对于 Satellite 中创建的所有 IPv6 子网，请将 DHCP Capsule 设置为空白。
3. 可选：如果主机和 DHCP 服务器由路由器分隔，请配置 DHCP 转发代理并指向 DHCP 服务器。
4. 在您置备的 Satellite 或 Capsule 上，将 grub2-efi 软件包更新至最新版本：

```
# satellite-maintain packages update grub2-efi
```

5. 同步 Red Hat Enterprise Linux 8 kickstart 存储库。

4.6. 使用 HTTP 代理配置 SATELLITE 服务器

使用以下步骤使用 HTTP 代理配置 Satellite。

4.6.1. 在 Satellite 中添加默认 HTTP 代理

如果您的网络使用 HTTP 代理，您可以将 Satellite 服务器配置为对 Red Hat Content Delivery Network (CDN)或其他内容源使用 HTTP 代理。尽可能使用 FQDN 而不是 IP 地址，以避免因为网络更改而丢失连接。

以下流程仅配置用于下载 Satellite 内容的代理。要使用 CLI 而不是 Satellite Web UI，请参阅 CLI 过程。

流程

1. 在 Satellite Web UI 中，进入到 Infrastructure > HTTP Proxies。
2. 单击 New HTTP Proxy。
3. 在 Name 字段中输入 HTTP 代理的名称。
4. 在 Url 字段中，以以下格式输入 HTTP 代理的 URL ：https://proxy.example.com:8080
5. 可选：如果需要身份验证，请在 Username 字段中输入要进行身份验证的用户名。
6. 可选：如果需要身份验证，请在 Password 字段中输入要进行身份验证的密码。
7. 要测试到代理的连接，请点 Test Connection。
8. 点 Submit。
9. 在 Satellite Web UI 中，进入到 Administer > Settings，然后点击 Content 选项卡。

10. **将 Default HTTP Proxy 设置设置为创建的 HTTP 代理。**

CLI 过程

1. 验证 **http_proxy、https_proxy 和 no_proxy** 变量没有被设置。

```
# unset http_proxy
# unset https_proxy
# unset no_proxy
```

2. **在 Satellite 中添加 HTTP 代理条目：**

```
# hammer http-proxy create --name=myproxy \
--url http://myproxy.example.com:8080  \
--username=proxy_username \
--password=proxy_password
```

3. **将 Satellite 配置为默认使用此 HTTP 代理：**

```
# hammer settings set --name=content_default_http_proxy --value=myproxy
```

4.6.2. 配置 SELinux 以确保在自定义端口上访问 Satellite

SELinux 确保了对特定端口的 Red Hat Satellite 和 Subscription Manager 的访问。对于 HTTP 缓存，TCP 端口为 8080、8118、8123 和 10001PROFILE-DESTINATION10010。如果您使用没有 SELinux 类型 http_cache_port_t 的端口，请完成以下步骤。

流程

1. **在 Satellite 上，要验证 SELinux 允许 HTTP 缓存的端口，请输入以下命令：**

```
# semanage port -l | grep http_cache
http_cache_port_t       tcp    8080, 8118, 8123, 10001-10010
[output truncated]
```

2. **要将 SELinux 配置为允许 HTTP 缓存的端口，如 8088，请输入如下命令：**

```
# semanage port -a -t http_cache_port_t -p tcp 8088
```

4.6.3. 将 HTTP 代理用于所有 Satellite HTTP 请求

如果您的 Satellite 服务器必须在阻止 HTTP 和 HTTPS 的防火墙后面，您可以配置代理与外部系统（包括计算资源）通信。

请注意，如果您使用计算资源进行置备，而您想要将不同的 HTTP 代理用于计算资源，则您为所有 Satellite 通信设置的代理优先于您为计算资源设置的代理。

流程

1. 在 Satellite Web UI 中，进入到 Administer > Settings。
2. 在 HTTP (S)代理 行中，选择 adjacent Value 列并输入代理 URL。
3. 点 tick 图标保存您的更改。

CLI 过程

- 输入以下命令：

```
# hammer settings set --name=http_proxy --value=Proxy_URL
```

4.6.4. 将主机从接收代理请求中排除

如果您将 HTTP 代理用于所有 Satellite HTTP 或 HTTPS 请求，您可以防止某些主机通过代理进行通信。

流程

1. 在 Satellite Web UI 中，进入到 Administer > Settings。
2. 在 HTTP (S)代理除了主机 行外，选择 adjacent Value 列，并输入您要从代理请求中排除的一个或多个主机的名称。
3. 点 tick 图标保存您的更改。

CLI 过程

- 输入以下命令：

```
# hammer settings set --name=http_proxy_except_list --value=[hostname1.hostname2...]
```

4.6.5. 重置 HTTP 代理

如果要重置当前的 HTTP 代理设置，请取消设置 Default HTTP Proxy 设置。

流程

1. 在 Satellite Web UI 中，进入到 Administer > Settings，然后点击 Content 选项卡。
2. 将 Default HTTP Proxy 设置设置为 no global default。

CLI 过程

- 将 content_default_http_proxy 设置设置为空字符串：

```
# hammer settings set --name=content_default_http_proxy --value=""
```

4.7. 在主机上启用电源管理

要使用智能平台管理接口(IPMI)或类似协议在主机上执行电源管理任务，您必须在 Satellite 服务器上启用基板管理控制器(BMC)模块。

先决条件

- 所有主机都必须具有 BMC 类型的网络接口。Satellite 服务器使用此 NIC 将适当的凭据传递给主机。如需更多信息，*请参阅管理主机* 中的 添加基板管理控制器(BMC)接口。

流程

- 要启用 BMC，请输入以下命令：

```
# satellite-installer --foreman-proxy-bmc "true" \
--foreman-proxy-bmc-default-provider "freeipmi"
```

4.8. 配置 DNS、DHCP 和 TFTP

您可以在 Satellite 环境中集中管理 DNS、DHCP 和 TFTP，也可以在禁用其 Satellite 维护后独立管理它们。您还可以在 Satellite 环境外部运行 DNS、DHCP 和 TFTP。

4.8.1. 在控制台中配置 DNS、DHCP 和 TFTP

要在 Satellite 服务器上配置 DNS、DHCP 和 TFTP 服务，请使用 satellite-installer 命令及适合您环境的选项。

对设置的任何更改都需要再次输入 satellite-installer 命令。您可以多次输入命令，每次使用更改后的值更新所有配置文件。

先决条件

- 确保以下信息可供您使用：
  - DHCP IP 地址范围
  - DHCP 网关 IP 地址
  - DHCP 名称服务器 IP 地址
  - DNS 信息
  - TFTP 服务器名称
- 在网络更改时，请使用 FQDN 而不是 IP 地址。
- 请联系您的网络管理员，以确保您有正确的设置。

流程

- 输入 **satellite-installer** 命令以及适合您的环境的选项。以下示例显示了配置完整置备服务：

```
# satellite-installer \
--foreman-proxy-dns true \
--foreman-proxy-dns-managed true \
--foreman-proxy-dns-zone example.com \
--foreman-proxy-dns-reverse 2.0.192.in-addr.arpa \
--foreman-proxy-dhcp true \
--foreman-proxy-dhcp-managed true \
--foreman-proxy-dhcp-range "192.0.2.100 192.0.2.150" \
--foreman-proxy-dhcp-gateway 192.0.2.1 \
--foreman-proxy-dhcp-nameservers 192.0.2.2 \
--foreman-proxy-tftp true \
--foreman-proxy-tftp-managed true \
--foreman-proxy-tftp-servername 192.0.2.3
```

您可以监控提示符中显示的 **satellite-installer** 命令的进度。您可以查看 **/var/log/foreman-installer/satellite.log** 中的日志。

其他资源

- 有关 **satellite-installer --scenario satellite** 命令的更多信息，请输入 **satellite-installer --scenario satellite --help**。

4.8.2. 为非受管网络禁用 DNS、DHCP 和 TFTP

如果要手动管理 **TFTP**、**DHCP** 和 **DNS** 服务，您必须防止 **Satellite** 在操作系统上维护这些服务，并禁用编配以避免 **DHCP** 和 **DNS** 验证错误。但是，**Satellite** 不会删除操作系统中的后端服务。

流程

1. 在 **Satellite** 服务器上输入以下命令：

```
# satellite-installer --foreman-proxy-dhcp false \
--foreman-proxy-dns false \
--foreman-proxy-tftp false
```

2. 在 **Satellite Web UI** 中，进入到 **Infrastructure > Subnets** 并选择子网。

3. 单击 **Capsules** 选项卡，再清除 **DHCP Capsule**、**TFTP Capsule** 和 反向 **DNS Capsule** 字

段。

4. 在 Satellite Web UI 中，进入到 Infrastructure > Domains 并选择域。

5. 清除 DNS Capsule 字段。

6. 可选：如果您使用由第三方提供的 DHCP 服务，请将 DHCP 服务器配置为传递以下选项：

```
Option 66: IP address of Satellite or Capsule
Option 67: /pxelinux.0
```

有关 DHCP 选项的更多信息，请参阅 RFC 2132。

注意

当没有为给定子网和域设置胶囊时，Satellite 不会执行编排。在启用或禁用 Capsule 关联时，如果预期的记录和配置文件不存在，现有主机的编配命令可能会失败。当关联一个 Capsule 以进行打开电源编配时，请确保现有 Satellite 主机所需的 DHCP 和 DNS 记录以及 TFTP 文件，以防止主机删除失败。

4.8.3. 其他资源

- 有关外部配置 DNS、DHCP 和 TFTP 的详情，请参考 *第 6 章 使用外部服务配置 Satellite 服务器*。

- 有关配置 DHCP、DNS 和 TFTP 服务的更多信息，请参阅 *置备主机 中的 配置网络服务* 。

4.9. 为出站电子邮件配置 SATELLITE 服务器

要从 Satellite 服务器发送电子邮件消息，您可以使用 SMTP 服务器或 sendmail 命令。

前提条件

- 已知的某些具有反垃圾邮件保护或问候功能的 SMTP 服务器会导致问题。要设置具有此类服务的传出电子邮件，可以安装和配置卫星服务器上的 vanilla SMTP 服务进行转发，或者使用

sendmail 命令。

流程

1. **在 Satellite Web UI 中，进入到 Administer > Settings。**

2. **单击 Email 选项卡，并将配置选项设置为与您首选的发送方法匹配。更改会立即生效。**

   a. **以下示例显示了使用 SMTP 服务器的配置选项：**

   表 4.1. 使用 SMTP 服务器作为发送方法

Name	示例值
交付方法	SMTP
SMTP 地址	*smtp.example.com*
SMTP 身份验证	login
SMTP HELO/EHLO 域	*example.com*
SMTP 密码	*password*
SMTP 端口	25
SMTP 用户名	*user@example.com*

   SMTP 用户名和 SMTP 密码 指定 SMTP 服务器的登录凭据。

   b. **以下示例使用 gmail.com 作为 SMTP 服务器：**

   表 4.2. 使用 gmail.com 作为 SMTP 服务器

Name	示例值
交付方法	SMTP
SMTP 地址	smtp.gmail.com

Name	示例值
SMTP 身份验证	plain
SMTP HELO/EHLO 域	smtp.gmail.com
SMTP 启用 StartTLS 自动	是
SMTP 密码	*password*
SMTP 端口	587
SMTP 用户名	*user*@gmail.com

c.

以下示例使用 sendmail 命令作为发送方法：

表 4.3. 使用 sendmail 作为发送方法

Name	示例值
交付方法	sendmail
Sendmail 位置	/usr/sbin/sendmail
Sendmail 参数	-i

出于安全考虑，Sendmail 位置和 Sendmail 参数设置都是只读的，只能在 /etc/foreman/settings.yaml 中设置。目前无法通过 satellite-installer 设置这两个设置。如需更多信息，请参阅 sendmail 1 man page。

3.

如果您决定使用 TLS 验证的 SMTP 服务器发送电子邮件，请执行以下步骤之一：

- **将 SMTP 服务器的 CA 证书标记为可信。要做到这一点，请在 Satellite 服务器上执行以下命令：**

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

其中 *mailca.crt* 是 SMTP 服务器的 CA 证书。

- 或者，在 Satellite Web UI 中，将 SMTP enable StartTLS auto 选项设置为 No。

4. 单击 Test email，将测试消息发送到用户的电子邮件地址，以确认配置是否正常工作。如果消息无法发送，Satellite Web UI 会显示错误。详情请查看 /var/log/foreman/production.log 的日志。

其他资源

- 有关为单个用户或用户组配置电子邮件通知的详情，请参考 管理 *Red Hat Satellite 中的配置电子邮件通知* 首选项。

4.10. 为 SATELLITE 配置备用 CNAME

您可以为 Satellite 配置备用 CNAME。如果您要将 Satellite Web 界面部署到与客户端系统用来连接到 Satellite 的不同域名上，这可能很有用。在安装胶囊并将主机注册到 Satellite 之前，您必须提前规划备用 CNAME 配置，以避免将新证书重新部署到主机。

4.10.1. 使用备用 CNAME 配置 Satellite

使用这个流程配置带有备用 CNAME 的 Satellite。请注意，默认 Satellite 证书和自定义证书用户的步骤有所不同。

对于默认 Satellite 证书用户

- 如果您使用默认 Satellite 证书安装了 Satellite，并希望使用备用 CNAME 配置 Satellite，请在 Satellite 上输入以下命令来生成带有额外 CNAME 的新默认 Satellite SSL 证书。

```
# satellite-installer --certs-cname alternate_fqdn --certs-update-server
```

- 如果您还没有安装 Satellite，您可以在 satellite-installer 命令中添加 **--certs-cname** *alternate_fqdn* 选项，以使用备用 CNAME 安装 Satellite。

对于自定义证书用户

如果您将 Satellite 与自定义证书一起使用，请在创建自定义证书时包括到自定义证书的替代 CNAME 记录。如需更多信息，请参阅为 Satellite 服务器创建自定义 SSL 证书。

4.10.2. 配置主机以使用备用 Satellite CNAME 进行内容管理

如果 Satellite 配置了备用 CNAME，您可以将主机配置为使用备用 Satellite CNAME 进行内容管理。为此，您必须在将主机注册到 Satellite 之前将主机指向备用 Satellite CNAME。您可以使用 bootstrap 脚本或手动进行此操作。

使用 bootstrap 脚本配置主机

在主机上，使用 **--server *alternate_fqdn.example.com*** 选项运行 bootstrap 脚本，将主机注册到备用 Satellite CNAME：

```
# ./bootstrap.py --server alternate_fqdn.example.com
```

手动配置主机

在主机上，编辑 **/etc/rhsm/rhsm.conf** 文件以更新 **hostname** 和 **baseurl** 设置以指向备用主机名，例如：

```
[server]
# Server hostname:
hostname = alternate_fqdn.example.com

content omitted

[rhsm]
# Content base URL:
baseurl=https://alternate_fqdn.example.com/pulp/content/
```

现在，您可以使用 subscription-manager 注册主机。

4.11. 使用自定义 SSL 证书配置 SATELLITE 服务器

默认情况下，Red Hat Satellite 使用自签名 SSL 证书来启用 Satellite 服务器、外部胶囊服务器和所有主机之间的加密通信。如果无法使用 Satellite 自签名证书，您可以将 Satellite 服务器配置为使用由外部证书颁发机构(CA)签名的 SSL 证书。

当使用自定义 SSL 证书配置 Red Hat Satellite 时，您必须满足以下要求：

- 您必须对 SSL 证书使用隐私增强型邮件(PEM)编码。
- 您不能将相同的 SSL 证书用于 Satellite 服务器和 Capsule 服务器。

- 同一 CA 必须为 Satellite 服务器和 Capsule 服务器签名证书。
- SSL 证书也不能是 CA 证书。
- SSL 证书必须包含与通用名称(CN)匹配的主题 alt name (SAN)条目。
- 在使用密钥用法扩展时，必须允许 SSL 证书。
- SSL 证书不能有短名称作为 CN。
- 您不能为私钥设置密码短语。

要使用自定义证书配置 Satellite 服务器，请完成以下步骤：

1. 第 4.11.1 节 “为 Satellite 服务器创建自定义 SSL 证书”
2. 第 4.11.2 节 “将自定义 SSL 证书部署到 Satellite 服务器”
3. 第 4.11.3 节 “将自定义 SSL 证书部署到主机”
4. 如果您的外部胶囊服务器注册到 Satellite 服务器，请使用自定义 SSL 证书进行配置。如需更多信息，请参阅安装 Capsule 服务器 中的 配置带有自定义 SSL 证书的 *Capsule 服务器*。

4.11.1. 为 Satellite 服务器创建自定义 SSL 证书

使用这个流程为 Satellite 服务器创建自定义 SSL 证书。如果您已有 Satellite 服务器的自定义 SSL 证书，请跳过此步骤。

流程

1. 要存储所有源证书文件，请创建一个只能被 root 用户访问的目录：

```
# mkdir /root/satellite_cert
```

2. 创建为证书签名请求(CSR)签名的私钥。

请注意，私钥必须未加密。如果您使用密码保护的私钥，请删除私钥密码。

如果您已有此 Satellite 服务器的私钥，请跳过这一步。

```
# openssl genrsa -out /root/satellite_cert/satellite_cert_key.pem 4096
```

3. 为 CSR 创建 /root/satellite_cert/openssl.cnf 配置文件并包含以下内容：

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
prompt = no

[ req_distinguished_name ]
commonName = satellite.example.com

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth, codeSigning, emailProtection
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = satellite.example.com
```

4. 可选：如果要向 CSR 添加可辨识名称(DN)详情，请在 [req_distinguished_name] 部分添加以下信息：

```
[req_distinguished_name]
CN = satellite.example.com
countryName =My_Country_Name (1)
stateOrProvinceName = My_State_Or_Province_Name (2)
localityName = My_Locality_Name (3)
organizationName = My_Organization_Or_Company_Name
organizationalUnitName = My_Organizational_Unit_Name (4)
```

(1)

两个字母代码

2

全名

3

全名（例如：New York）

4

负责证书的部门（示例：IT 部门）

5. 生成 CSR：

```
# openssl req -new \
-key /root/satellite_cert/satellite_cert_key.pem \ 1
-config /root/satellite_cert/openssl.cnf \ 2
-out /root/satellite_cert/satellite_cert_csr.pem 3
```

1

私钥的路径

2

配置文件的路径

3

要生成的 CSR 的路径

6. 将证书签名请求发送到证书颁发机构(CA)。同一 CA 必须为 Satellite 服务器和 Capsule 服务器签名证书。

提交请求时，指定证书的寿命。发送证书请求的方法会有所不同，因此请查阅 CA 查看首选方法。为了响应请求，您可以在单独的文件中接收 CA 捆绑包和签名证书。

4.11.2. 将自定义 SSL 证书部署到 Satellite 服务器

使用这个流程将 Satellite 服务器配置为使用证书颁发机构签名的自定义 SSL 证书。katello-certs-check 命令验证输入证书文件，并返回将自定义 SSL 证书部署到 Satellite 服务器所需的命令。

重要

不要将 SSL 证书或 .tar 捆绑包存储在 /tmp 或 /var/tmp 目录中。操作系统定期从这些目录中删除文件。因此，satellite-installer 在启用功能或升级 Satellite 服务器时无法执行。

流程

1. 验证自定义 SSL 证书输入文件。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 \
-c /root/satellite_cert/satellite_cert.pem \ 1
-k /root/satellite_cert/satellite_cert_key.pem \ 2
-b /root/satellite_cert/ca_cert_bundle.pem 3
```

1. 由证书颁发机构签名的 Satellite 服务器证书文件的路径。
2. 用于为 Satellite 服务器证书签名的私钥的路径。
3. 证书颁发机构捆绑包的路径。

如果命令成功，它会返回两个 satellite-installer 命令，其中之一必须用于部署证书到 Satellite 服务器。

katello-certs-check的输出示例

```
Validation succeeded.

To install the Red Hat Satellite Server with the custom certificates, run:
```

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

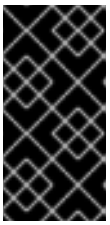
To update the certificates on a currently running Red Hat Satellite installation, run:

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

请注意，不得访问或修改 /root/ssl-build。

2. 根据您的要求，在 katello-certs-check 命令的输出中，输入 satellite-installer 命令，该命令使用自定义 SSL 证书或更新当前运行的 Satellite 上的证书。

如果您不确定要运行的命令，您可以通过检查文件 /etc/foreman-installer/scenarios.d/.installed 来验证是否安装了 Satellite。如果文件存在，请运行第二个 satellite-installer 命令来更新证书。



重要

在部署证书后，Satellite-installer 需要证书存档文件。不要修改或删除它。例如，升级 Satellite 服务器时需要这样做。

3. 在可访问 Satellite 服务器的计算机上，导航到以下 URL ：

4. 在您的浏览器中，查看证书详情以验证部署的证书。

4.11.3. 将自定义 SSL 证书部署到主机

将 Satellite 配置为使用自定义 SSL 证书后，您必须将证书部署到注册到 Satellite 的主机。

流程

- 更新每个主机上的 SSL 证书：

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

4.12. 在 SATELLITE 中使用外部数据库

作为 Red Hat Satellite 的安装过程的一部分，satellite-installer 命令会在与 Satellite 相同的服务器上安装 PostgreSQL 数据库。在某些 Satellite 部署中，使用外部数据库而不是默认的本地数据库可帮助进行服务器负载。

红帽不提供对外部数据库维护的支持或工具。这包括备份、升级和数据库调优。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。

要为 Satellite 创建和使用外部数据库，您必须完成以下步骤：

1. 第 4.12.2 节 “为外部数据库准备主机”.准备托管外部数据库的 Red Hat Enterprise Linux 8 服务器。
2. 第 4.12.3 节 “安装 PostgreSQL”.使用 Satellite 的数据库准备 PostgreSQL，使用拥有他们的专用用户 Candlepin 和 Pulp。
3. 第 4.12.4 节 “将 Satellite 服务器配置为使用外部数据库”.编辑 satellite-installer 的参数以指向新数据库，并运行 satellite-installer。

4.12.1. PostgreSQL 作为外部数据库注意事项

Foreman、Katello 和 Candlepin 使用 PostgreSQL 数据库。如果要将 PostgreSQL 用作外部数据库，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

- 在 Satellite 上增加可用内存和可用 CPU
- 在 PostgreSQL 数据库上设置 shared_buffers 的灵活性，使其没有与 Satellite 上的其他服务干扰的风险

- 在不影响 Satellite 操作的情况下灵活地调整 PostgreSQL 服务器系统

外部 PostgreSQL 的缺点

- 增加部署复杂性，使故障排除变得更加困难
- 外部 PostgreSQL 服务器是一个额外的系统来修补和维护
- 如果 Satellite 或 PostgreSQL 数据库服务器都存在硬件或存储故障，则 Satellite 无法正常工作
- 如果 Satellite 服务器和数据库服务器之间有延迟，则性能可能会下降

如果您怀疑 Satellite 上的 PostgreSQL 数据库导致性能问题，请在 Satellite 6 中使用信息：如何启用 postgres 查询日志记录来检测运行较慢的查询，以确定您是否有缓慢的查询。超过一秒的查询通常是由于大型安装出现性能问题导致的，而迁移到外部数据库可能并不有所帮助。如果您的查询缓慢，请联系红帽支持团队。

4.12.2. 为外部数据库准备主机

使用最新的 Red Hat Enterprise Linux 8 安装一个全新的置备系统，以托管外部数据库。

Red Hat Enterprise Linux 的订阅不提供将 Satellite 与外部数据库的正确服务级别协议。您还必须将 Satellite 订阅附加到要用于外部数据库的基本操作系统。

先决条件

- 准备的主机必须满足 Satellite 的存储要求。

流程

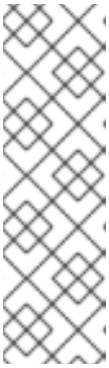
1. 按照 附加 Satellite Infrastructure 订阅 中的说明，将 Satellite 订阅附加到您的服务器。

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-6.15-for-rhel-8-x86_64-rpms \
--enable=satellite-maintenance-6.15-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，因为这些模块被设置为 **Red Hat Enterprise Linux 8** 上的默认模块版本。模块 **satellite:el8** 具有模块 **postgresql:12** 和 **ruby:2.7** 的依赖项，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** 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**。

4.12.3. 安装 PostgreSQL

您只能在内部数据库安装过程中安装 **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 postgresql-contrib
```

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 的默认配置才能使用 Satellite。基础推荐的外部数据库配置调整如下：

- **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. **在外部 PostgreSQL 服务器上打开 postgresql 端口：**

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

9. **使更改持久：**

```
# firewall-cmd --runtime-to-permanent
```

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

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

11. **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;
```

12. **连接到 Pulp 数据库：**

```
postgres=# \c pulpcore
You are now connected to database "pulpcore" as user "postgres".
```

13. **创建 hstore 扩展：**

```
pulpcore=# CREATE EXTENSION IF NOT EXISTS "hstore";
CREATE EXTENSION
```

14. **退出 postgres 用户：**

```
# \q
```

15. **从 Satellite 服务器中，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"
```

4.12.4. 将 Satellite 服务器配置为使用外部数据库

使用 satellite-installer 命令，将 Satellite 配置为连接到外部 PostgreSQL 数据库。

前提条件

- 您已在 Red Hat Enterprise Linux 服务器中安装并配置 PostgreSQL 数据库。

流程

1. 要为 Satellite 配置外部数据库，请输入以下命令：

```
# satellite-installer --scenario satellite \
--foreman-db-database foreman \
--foreman-db-host postgres.example.com \
--foreman-db-manage false \
--foreman-db-password Foreman_Password \
--foreman-proxy-content-pulpcore-manage-postgresql false \
--foreman-proxy-content-pulpcore-postgresql-db-name pulpcore \
--foreman-proxy-content-pulpcore-postgresql-host postgres.example.com \
--foreman-proxy-content-pulpcore-postgresql-password Pulpcore_Password \
--foreman-proxy-content-pulpcore-postgresql-user pulp \
--katello-candlepin-db-host postgres.example.com \
--katello-candlepin-db-name candlepin \
--katello-candlepin-db-password Candlepin_Password \
--katello-candlepin-manage-db false
```

要为这些外部数据库启用安全套接字层(SSL)协议，请添加以下选项：

```
--foreman-db-root-cert <path_to_CA>
--foreman-db-sslmode verify-full
--foreman-proxy-content-pulpcore-postgresql-ssl true
--foreman-proxy-content-pulpcore-postgresql-ssl-root-ca <path_to_CA>
--katello-candlepin-db-ssl true
--katello-candlepin-db-ssl-ca <path_to_CA>
--katello-candlepin-db-ssl-verify true
```

第 5 章 配置外部身份验证

通过使用外部身份验证，您可以从外部身份提供程序中的用户组成员资格派生用户和用户组权限。使用外部身份验证时，您不必在 Satellite 服务器上手动创建这些用户并手动维护其组成员资格。如果外部来源不提供电子邮件，将在首次通过 Satellite Web UI 登录期间请求。

重要用户和组群帐户信息

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

如果您的用户和组帐户同时存在于 /etc/passwd 和 /etc/group 文件中，您的系统不会受到此冲突的影响。例如，要检查 /etc/passwd 和 /etc/group 文件中是否存在 puppet、apache、foreman 和 foreman-proxy 组的条目，请输入以下命令：

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

配置外部身份验证的情况

Red Hat Satellite 支持以下配置外部身份验证的一般场景：

- *使用轻量级目录访问协议(* LDAP)服务器作为外部身份提供程序。LDAP 是一组开放协议，用于通过网络访问集中存储的信息。使用 Satellite，您可以通过 Satellite Web UI 完全管理 LDAP。更多信息请参阅 第 5.1 节 “使用 LDAP”。虽然您可以使用 LDAP 连接到红帽身份管理或 AD 服务器，但设置不支持在 Satellite 的 Web UI 中使用 Kerberos 进行服务器发现、跨林信任或单点登录。
- 使用红帽身份管理服务器作为外部身份提供程序。Red Hat Identity Management 负责管理个别身份、其在网络环境中使用的凭证和特权。使用红帽身份管理的配置无法仅使用 Satellite Web UI 来完成，并且需要一些与 CLI 的交互。如需更多信息，请参阅 第 5.2 节 “使用红帽身份管理”。
- 通过跨林信任 Kerberos 信任作为外部身份提供程序，使用 *Active Directory* (AD)与红帽身份管理集成。如需更多信息，请参阅 第 5.3.5 节 “具有跨林信任的活动目录”。
- 使用红帽单点登录作为 OpenID 提供程序，以向 Satellite 进行外部身份验证。更多信息请参阅 第 5.9 节 “使用红帽单点登录身份验证配置 Satellite”。
-

使用红帽单点登录作为 OpenID 提供程序，用于通过 TOTP 向 Satellite 进行外部身份验证。更多信息请参阅 第 5.10 节 “使用 TOTP 配置 Red Hat Single Sign-On 身份验证”。

除了提供对 Satellite 服务器的访问权限外，也可通过 Satellite 置备的主机也可以与红帽身份管理域集成。Red Hat Satellite 有一个域功能，它会自动管理注册到域或域提供程序的任何系统的生命周期。如需更多信息，请参阅 第 5.8 节 “置备的主机的外部身份验证”。

表 5.1. 身份验证概述

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

5.1. 使用 LDAP

Satellite 支持使用一个或多个 LDAP 目录的 LDAP 身份验证。

如果您需要 Red Hat Satellite 使用 TLS 建立安全 LDAP 连接(LDAPS)，首先获取您连接的 LDAP 服务器使用的证书，并将其标记为可信到 Satellite 服务器的基本操作系统上，如下所述。如果您的 LDAP 服务器使用带有中间证书颁发机构的证书链，则链中的所有 root 和中间证书都必须被信任，以确保获取所有证书。如果您目前不需要安全的 LDAP，请继续 第 5.1.2 节 “将 Red Hat Satellite 配置为使用 LDAP”。

重要

用户不能同时使用 Red Hat Identity Management 和 LDAP 作为身份验证方法。用户使用某种方法进行身份验证后，他们无法使用其他方法。

要更改用户的身份验证方法，您必须从 Satellite 中删除自动创建的用户。

有关使用 Red Hat Identity Management 作为验证方法的详情，请参考 第 5.2 节 “使用红帽身份管理”。

5.1.1. 为安全 LDAP 配置 TLS

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

流程

1. 从 LDAP 服务器获取证书。

   a. 如果您使用 Active Directory 证书服务，请使用以 Base-64 编码的 X.509 格式导出企业 PKI CA 证书。有关从 Active Directory 服务器创建和导出 CA 证书的信息，请参阅 如何通过 Satellite 上的 TLS 配置活动目录身份验证。

   b. 将 LDAP 服务器证书下载到卫星服务器上的临时位置，并在完成后删除它。

   例如： /tmp/example.crt。文件名扩展 .cer 和 .crt 只是约定，可以引用 DER 二进制或 PEM ASCII 格式证书。

2. 信任 LDAP 服务器的证书。

   Satellite 服务器要求 LDAP 身份验证的 CA 证书是 /etc/pki/tls/certs/ 目录中的单个文件。

   a. 使用 install 命令将导入的证书安装到具有正确权限的 /etc/pki/tls/certs/ 目录中：

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

   b. 以 root 用户身份输入以下命令，以信任从 LDAP 服务器获取的 *example.crt* 证书：

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

   c. 重启 httpd 服务：

   ```
   # systemctl restart httpd
   ```

5.1.2. 将 Red Hat Satellite 配置为使用 LDAP

在 Satellite Web UI 中，将 Satellite 配置为使用 LDAP。

请注意，如果您在 Satellite Web UI 上需要 Kerberos 单点登录功能，您应该改为使用 Red Hat Identity Management 和 AD 外部身份验证。如需更多信息，请参阅：

- 第 5.2 节 “使用红帽身份管理”
- 第 5.3 节 “使用 Active Directory”

流程

1. 将网络信息系统(NIS)服务布尔值设置为 true，以防止 SELinux 停止传出的 LDAP 连接：

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

2. 在 Satellite Web UI 中，进入到 Administer > Authentication Sources。
3. 单击 Create LDAP Authentication Source。
4. 在 LDAP 服务器 选项卡上，输入 LDAP 服务器的名称、主机名、端口和服务器类型。默认端口是 389，默认服务器类型是 POSIX （根据身份验证服务器的类型，也可以选择 FreeIPA 或 Active Directory）。对于 TLS 加密连接，请选择 LDAPS 复选框来启用加密。端口应更改为 636，这是 LDAPS 的默认设置。
5. 在帐户选项卡上，输入帐户信息和域名详细信息。有关描述和示例，请参阅 第 5.1.3 节 “LDAP 设置的描述”。
6. 在 属性映射 选项卡上，将 LDAP 属性映射到 Satellite 属性。您可以映射登录名称、名字、姓氏、电子邮件地址和照片属性。如需示例，请参阅 第 5.1.4 节 “LDAP 连接的设置示例”。
7. 在 位置 选项卡上，从左侧表中选择位置。所选位置分配给从 LDAP 身份验证源创建的用户，并在首次登录后可用。
8.

在 组织 选项卡上，从左侧表中选择组织。所选机构被分配给从 LDAP 身份验证源创建的用户，并在用户首次登录后可用。

9. 点 Submit。

10. 为 LDAP 用户配置新帐户：

- 如果您没有选择 Automatically Create Accounts In Satellite 复选框，请参阅 *管理 Red Hat Satellite* 中的 创建用户 来手动创建用户帐户。

- 如果您选择了 Automatically Create Accounts In Satellite 复选框，LDAP 用户现在可以使用其 LDAP 帐户和密码登录 Satellite。第一次登录后，卫星管理员必须手动将角色分配给它们。有关在 Satellite 中分配用户帐户的更多信息，请参阅管理 *Red Hat Satellite* 中的为用户分配角色。https://access.redhat.com/documentation/zh-cn/red_hat_satellite/6.15/html-single/administering_red_hat_satellite/index#Assigning_Roles_to_a_User_admin

5.1.3. LDAP 设置的描述

下表提供了 帐户 选项卡中每个设置的描述。

表 5.2. 帐户标签页设置

设置	描述
帐户	对 LDAP 服务器具有读取访问权限的 LDAP 帐户的用户名。如果服务器允许匿名读取，则不需要用户名，否则使用用户对象的完整路径。例如： `uid=$login,cn=users,cn=accounts,dc=example,dc=com` **$login** 变量将登录页面中输入的用户名存储为字面字符串。在变量扩展时访问该值。 变量无法从 LDAP 源用于外部用户组，因为 Satellite 需要检索组列表，而无需用户登录。使用匿名或专用服务用户。
帐户密码	帐户用户名 字段中定义的用户的 LDAP 密码。如果帐户用户名 使用 **$login** 变量，则此字段可保持空白。
基本 DN	LDAP 目录的顶级域名。
组基本 DN	包含组的 LDAP 目录树的顶级域名。

设置	描述
LDAP 过滤器	用于限制 LDAP 查询的过滤器。
在 Satellite 中自动创建帐户	如果选中此复选框，Satellite 会在首次登录 Satellite 时为 LDAP 用户创建用户帐户。第一次登录后，卫星管理员必须手动将角色分配给它们。请参阅 *管理 Red Hat Satellite 中的为用户分配角色，以在 Satellite* 中分配适当的用户帐户。https://access.redhat.com/documentation/zh-cn/red_hat_satellite/6.15/html-single/administering_red_hat_satellite/index#Assigning_Roles_to_a_User_admin
usergroup Sync	如果选择了这个选项，则用户的用户组成员资格会在用户登录时自动同步，这样可确保成员资格始终保持最新状态。如果清除此选项，Satellite 依赖于 cron 作业定期同步组成员资格（默认为 30 分钟）。如需更多信息，请参阅 第 5.4 节 “配置外部用户组”。

5.1.4. LDAP 连接的设置示例

下表显示了不同类型的 LDAP 连接的示例设置。以下示例使用了一个名为 *redhat* 的专用服务帐户，该帐户对用户和组条目具有 bind、read 和 search 权限。请注意，LDAP 属性名称区分大小写。

表 5.3. Active Directory、Free IPA 或 Red Hat Identity Management 和 POSIX LDAP 连接的设置示例

设置	Active Directory	freeipa 或 Red Hat Identity Management	POSIX (OpenLDAP)
帐户	DOMAIN\redhat	uid=redhat,cn=users,cn=accounts,dc=example,dc=com	uid=redhat,ou=users,dc=example,dc=com
帐户密码	P@ssword	-	-
基本 DN	DC=example,DC=COM	dc=example,dc=com	dc=example,dc=com
组基本 DN	CN=Users,DC=example,DC=com	cn=groups,cn=accounts,dc=example,dc=com	cn=employee,ou=userclass,dc=example,dc=com
登录名称属性	userPrincipalName	uid	uid
名字属性	givenName	givenName	givenName
姓氏属性	sn	sn	sn
电子邮件地址属性	mail	mail	mail
photo 属性	thumbnailPhoto	-	-

注意

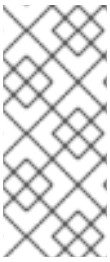
userPrincipalName 允许在用户名中使用空格。登录名称属性 sAMAccountName（在上表中未列出）提供与传统 Microsoft 系统向后兼容性。sAMAccountName 不允许在用户名中使用空格。

5.1.5. LDAP 过滤器示例

作为管理员，您可以创建 LDAP 过滤器，将特定用户的访问权限限制到 Satellite。

表 5.4. 允许特定用户登录的过滤器示例

用户	Filter
User1	(distinguishedName=cn=User1,cn=Users,dc=domain,dc=example)
User1、User3	(memberOf=cn=Group1,cn=Users,dc=domain,dc=example)
User2, User3	(memberOf=cn=Group2,cn=Users,dc=domain,dc=example)
User1, User2, User3	(|(memberOf=cn=Group1,cn=Users,dc=domain,dc=example) (memberOf=cn=Group2,cn=Users,dc=domain,dc=example))
User1, User2, User3	(memberOf:1.2.840.113556.1.4.1941:=cn=Users,dc=domain,dc=example)



注意

组 Users 是包含组 Group1 和 Group2 的嵌套组。如果要过滤嵌套组中的所有用户，您必须在嵌套组名称前添加 memberOf:1.2.840.113556.1.4.1941:=。请参阅上表中的最后一个示例。

LDAP 目录结构

示例中的过滤器使用的 LDAP 目录结构：

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

LDAP 组成员身份

示例中使用的过滤器的组成员资格：

组	成员
Group1	User1、User3
Group2	User2, User3

5.2. 使用红帽身份管理

本节介绍如何将 Satellite 服务器与红帽身份管理服务器集成，以及如何启用基于主机的访问控制。

注意

您可以将 Red Hat Identity Management 附加到外部身份验证源，而无需单点登录支持。如需更多信息，请参阅 第 5.1 节 “使用 LDAP”。

重要

用户不能同时使用 Red Hat Identity Management 和 LDAP 作为身份验证方法。用户使用某种方法进行身份验证后，他们无法使用其他方法。

要更改用户的身份验证方法，您必须从 Satellite 中删除自动创建的用户。

先决条件

- Satellite 服务器的基本操作系统必须由您机构的红帽身份管理管理员注册在红帽身份管理域中。

本章中的示例假定在红帽身份管理和 Satellite 配置之间分离。但是，如果您拥有这两个服务器的管理员特权，您可以配置 Red Hat Identity Management，如 Red Hat Enterprise Linux 8 安装身份管理指南 所述。

5.2.1. 在 Satellite 服务器中配置红帽身份管理身份验证

在 Satellite CLI 中，首先在 Red Hat Identity Management 服务器上创建主机条目来配置红帽身份管理身份验证。

流程

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

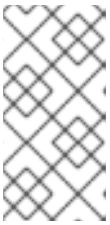
```
# kinit admin
```

2. 要验证您是否已通过身份验证，请输入以下命令：

```
# klist
```

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

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



注意

生成的一次性密码必须在客户端上使用，以完成 Red Hat Identity Management-enrollment。

有关主机配置属性的更多信息，请参阅 配置和管理身份管理 中的 IdM LDAP *中的主机条目*。

4. 为 Satellite 服务器创建 HTTP 服务，例如：

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

有关管理服务的更多信息，请参阅 Red Hat Enterprise Linux 8 访问身份管理服务指南。

5. 在 Satellite 服务器上安装 IPA 客户端：

警告

此命令可能会在安装软件包的过程中重启 Satellite 服务。有关在 Satellite 上安装和更新软件包的更多信息，请参阅管理 Red *Hat Satellite 中的在 Satellite 服务器的基本操作系统或 Capsule Server 上* 管理软件包。

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

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

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

将 *OTP* 替换为红帽身份管理管理员提供的一次性密码。

7. 使用以下命令之一将 Red Hat Identity Management 设置为身份验证供应商：

- 如果您只想启用对 Satellite Web UI 的访问，而不是 Satellite API，请输入：

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

- 如果要启用 Satellite Web UI 和 Satellite API 的访问，请输入：

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

警告

启用访问 Satellite API 和 Satellite Web UI 可能会导致安全问题。在 IdM 用户通过输入 kinit *user_name* 接收 Kerberos 票据授予票(TGT)后，攻击者可以获取 API 会话。即使用户之前没有在任何位置输入 Satellite 登录凭据，如浏览器中，也可以进行攻击。

8. 重启 Satellite 服务：

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

外部用户可以使用他们的红帽身份管理凭证登录 Satellite。现在，他们可以选择使用其用户名和密码直接登录到 Satellite 服务器，或者利用配置的 Kerberos 单点登录并在其客户端机器上获取票据并自动登录。也支持使用一次性密码(2FA OTP)进行双因素身份验证。

5.2.2. 配置基于主机的身份验证控制

HBAC 规则定义 Red Hat Identity Management 用户可以访问哪些机器。您可以在 Red Hat Identity Management 服务器上配置 HBAC，以防止所选用户访问 Satellite 服务器。通过这种方法，您可以防止 Satellite 为不允许登录的用户创建数据库条目。有关 HBAC 的更多信息，请参阅管理 IdM 用户、组、主机和访问控制规则指南。

在 Red Hat Identity Management 服务器上，配置基于主机的身份验证控制(HBAC)。

流程

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

```
# kinit admin
```

2. 要验证您是否已通过身份验证，请输入以下命令：

```
# klist
```

3. 在 Red Hat Identity Management 服务器上创建 HBAC 服务和规则，并将它们链接在一起。以下示例使用 PAM 服务名称 ***satellite-prod***。在 Red Hat Identity Management 服务器上执行以下命令：

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

4. 添加有权访问服务 **satellite-prod** 的用户，以及 Satellite 服务器的主机名：

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

或者，可以将主机组和用户组添加到 ***allow_satellite_prod*** 规则中。

5. 要检查规则的状态，请执行：

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

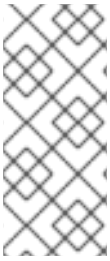
6. 确保 Red Hat Identity Management 服务器上禁用了 allow_all 规则。有关如何在不中断其他服务的情况下进行此操作的说明，请参阅红帽客户门户网站中的 如何在 IdM 中配置 HBAC 规则。

7. 配置红帽身份管理与 Satellite 服务器集成，如 第 5.2.1 节 “在 Satellite 服务器中配置红帽身份管理身份验证” 所述。在 Satellite 服务器上，将 PAM 服务定义为 **root** ：

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

5.3. 使用 ACTIVE DIRECTORY

本节介绍如何使用直接 Active Directory (AD)作为 Satellite 服务器的外部身份验证源。



注意

您可以将 Active Directory 附加到没有单点登录支持的外部身份验证源。更多信息请参阅 第 5.1 节 “使用 LDAP”。有关示例配置，请参阅 如何在 Satellite 上使用 TLS 配置 Active Directory 身份验证。

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

- 将 Satellite 服务器注册到 Active Directory 服务器，如 第 5.3.2 节 “使用 AD 服务器注册 Satellite 服务器” 所述。
- 配置直接 Active Directory 与 GSS-proxy 集成，如 第 5.3.3 节 “配置与 GSS-proxy 的直接 AD 集成” 所述。

5.3.1. GSS-Proxy

Apache 中 Kerberos 身份验证的传统进程需要 Apache 进程对 keytab 文件具有读访问权限。GSS-Proxy 允许您通过删除对 keytab 文件的访问同时保留 Kerberos 身份验证功能，为 Apache 服务器实施更严格的权限分离。当使用 AD 作为 Satellite 的外部身份验证源时，建议实施 GSS-proxy，因为 keytab 文件中的密钥与主机密钥相同。

在作为您的 Satellite 服务器基本操作系统的 Red Hat Enterprise Linux 上执行以下步骤。对于本节中的示例，*EXAMPLE.ORG* 是 AD 域的 Kerberos 域。通过完成这些步骤，属于 EXAMPLE.ORG 域的用户可以登录到 Satellite 服务器。

5.3.2. 使用 AD 服务器注册 Satellite 服务器

在 Satellite CLI 中，将 Satellite 服务器注册到 Active Directory 服务器。

先决条件

- 已安装 GSS-proxy 和 nfs-utils。

安装 GSS-proxy 和 nfs-utils：

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

流程

1. **安装所需的软件包：**

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

2. **将 Satellite 服务器注册到 AD 服务器。您可能需要具有管理员权限才能执行以下命令：**

```
# realm join -v EXAMPLE.ORG --membership-software=samba -U Administrator
```

注意

您必须使用 Samba 客户端软件注册 AD 服务器在 第 5.3.3 节 “配置与 GSS-proxy 的直接 AD 集成” 中创建 HTTP keytab。

5.3.3. 配置与 GSS-proxy 的直接 AD 集成

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

先决条件

- **Satellite 注册到 Active Directory 服务器。更多信息请参阅 第 5.3.2 节 “使用 AD 服务器注册 Satellite 服务器”。**

流程

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

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

2. **在 default.conf 文件中添加以下内容：**

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

3. 使用以下内容创建 /etc/net-keytab.conf 文件：

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

4. 确定 Apache 用户的有效用户 ID：

```
# id apache
```

Apache 用户不能访问 keytab 文件。

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

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

6. 创建 keytab 条目：

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

7. 在 Satellite 中启用 IPA 身份验证：

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

8. 启动并启用 gssproxy 服务：

```
# systemctl restart gssproxy
# systemctl enable --now gssproxy
```

9. 要将 Apache 服务器配置为使用 gssproxy 服务，请创建一个 systemd 置入文件，并将以

下内容添加到其中：

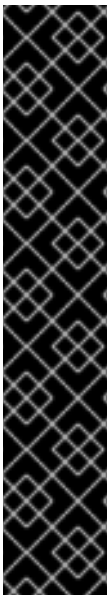
```
# mkdir -p /etc/systemd/system/httpd.service.d/
# vi /etc/systemd/system/httpd.service.d/gssproxy.conf
[Service]
Environment=GSS_USE_PROXY=1
```

10. 对服务应用更改：

```
# systemctl daemon-reload
```

11. 启动并启用 **httpd** 服务：

```
# systemctl restart httpd
```



重要

通过直接 AD 集成，没有通过 Red Hat Identity Management 的 HBAC。另外，您可以使用组策略对象(GPO)来让管理员在 AD 环境中集中管理策略。要确保正确的 GPO 到 PAM 服务映射，请将以下 SSSD 配置添加到 /etc/sssd/sssd.conf 中：

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

在这里，*foreman* 是 PAM 服务名称。如需有关 GPO 的更多信息，请参阅 *将 RHEL 系统直接与 Windows 目录服务器集成* 中的 SSSD 如何解释 GPO 访问控制规则。

验证

验证 SSO 是否按预期工作。

运行 Apache 服务器时，如果客户端具有有效的 Kerberos 票据，则对服务器发出 HTTP 请求的用户会被验证。

1. 使用以下命令，检索 LDAP 用户的 Kerberos 票据：

```
# kinit ldapuser
```

2. 使用以下命令查看 Kerberos 票据：

```
# klist
```

3. 使用以下命令，查看成功基于 SSO 的身份验证的输出：

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

这会返回以下响应：

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

5.3.4. Web 浏览器中的 Kerberos 配置

有关配置 Firefox 的详情，请参考 *Red Hat Enterprise Linux 在 RHEL 中配置身份验证和授权* 指南中的 配置 Firefox 以为单点登录使用 Kerberos。

如果您使用 Internet Explorer 浏览器，请将 Satellite 服务器添加到本地 I intranet 或 Trusted 站点列表中，然后打开 *Enable Integrated Windows Authentication* 设置。详情请查看 Internet Explorer 文档。

5.3.5. 具有跨林信任的活动目录

Kerberos 可以创建 跨林信任，以定义两个其他独立域林之间的关系。域林是域的层次结构，AD 和红帽身份管理均构成了林。AD 和 Red Hat Identity Management 之间启用了信任关系，AD 用户可以使用一组凭证访问 Linux 主机和服务。如需有关跨林信任的更多信息，请参阅在 *Red Hat Enterprise Linux 规划身份管理* 中的 规划 IdM 和 AD 之间的跨林信任。

从 Satellite 的角度来看，配置过程与没有配置跨林信任的情况下与红帽身份管理服务器集成相同。Satellite 服务器必须在 IdM 域中注册，并集成，如 第 5.2 节 “使用红帽身份管理” 所述。

5.3.6. 将 Red Hat Identity Management 服务器配置为使用跨林信任

在 Red Hat Identity Management 服务器上，将服务器配置为使用 跨林信任。

流程

1. 启用 HBAC ：

   a. 创建一个外部组，并将 AD 组添加到其中。

   b. 将新的外部组添加到 POSIX 组。

   c. 在 HBAC 规则中使用 POSIX 组。

2. 配置 sssd 以传输 AD 用户的额外属性。

   - 将 AD 用户属性添加到 /etc/sssd/sssd.conf 中的 *nss* 和 *domain* 部分。例如：

```
[nss]
user_attributes=+mail, +sn, +givenname
[domain/EXAMPLE.com]
...
krb5_store_password_if_offline = True
ldap_user_extra_attrs=email:mail, lastname:sn, firstname:givenname

[ifp]
allowed_uids = ipaapi, root
user_attributes=+email, +firstname, +lastname
```

   - 验证 AD 属性值。

```
# dbus-send --print-reply --system --dest=org.freedesktop.sssd.infopipe
/org/freedesktop/sssd/infopipe org.freedesktop.sssd.infopipe.GetUserAttr string:ad-
user@ad-domain array:string:email,firstname,lastname
```

5.4. 配置外部用户组

Satellite 不会自动将外部用户与其用户组关联。您必须创建一个与 Satellite 上外部源相同的用户组。然后，外部用户组的成员会自动成为 Satellite 用户组的成员并接收关联的权限。

外部用户组的配置取决于外部身份验证的类型。

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

先决条件

- 如果您使用 LDAP 服务器，请将 Satellite 配置为使用 LDAP 身份验证。如需更多信息，请参阅 第 5.1 节 “使用 LDAP”。

  使用 LDAP 源的外部用户组时，您无法使用 $login 变量作为帐户用户名的替换。您必须使用匿名或专用服务用户。

- 如果您使用 Red Hat Identity Management 或 AD 服务器，请将 Satellite 配置为使用 Red Hat Identity Management 或 AD 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*。

- 确保至少有一个外部用户第一次进行身份验证。

- 保留您要使用的外部组名称的一份副本。要查找外部用户的组成员资格，请输入以下命令：

```
# id username
```

流程

1. 在 Satellite Web UI 中，进入到 Administer > User Groups，然后点 Create User Group。

2. 指定新用户组的名称。不要选择任何用户，以避免在刷新外部用户组时自动添加用户。

3. 点 Roles 选项卡，再选择您要分配给用户组的角色。或者，选择 Administrator 复选框来分配所有可用权限。

4. 单击 External groups 选项卡，然后单击 Add external user group，然后从 Auth source 下拉菜单中选择身份验证源。

   在 Name 字段中指定外部组的名称。

5. 点 Submit。

5.5. 为 LDAP 刷新外部用户组

要将 LDAP 源设置为在用户登录时自动同步用户组成员资格，请在 Auth Source 页面中选择 Usergroup Sync 选项。如果未选中此选项，则默认情况下，LDAP 用户组将通过调度的 cron 作业自动刷新一次，每 30 分钟同步 LDAP 身份验证源。

如果 LDAP 身份验证源中的用户组在调度任务之间的时间变化，则可以将该用户分配给不正确的外部用户组。这会在调度任务运行时自动修正。

使用这个流程手动刷新 LDAP 源。

流程

1. 在 Satellite Web UI 中，进入到 Administer > Usergroups 并选择用户组。
2. 在 External Groups 选项卡上，单击所需用户组右侧的 Refresh。

CLI 过程

- 输入以下命令：

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

5.6. 为 RED HAT IDENTITY MANAGEMENT 或 AD 刷新外部用户组

只有在组成员登录到 Satellite 时，才会刷新基于红帽身份管理或 AD 的外部用户组。在 Satellite Web UI 中无法更改外部用户组的用户成员资格，此类更改会在下一个组刷新时被覆盖。

5.7. 配置 HAMMER CLI 以使用 RED HAT IDENTITY MANAGEMENT 用户身份验证

本节论述了如何配置 Satellite Hammer 命令行界面(CLI)工具以使用 Red Hat Identity Management (IdM)来验证用户。

先决条件

- 您使用 Hammer 登录到您要从中访问 Satellite 的主机。

流程

1. 通过在 foreman 参数中添加 :use_sessions: true 行，在 ~/.hammer/cli.modules.d/foreman.yml Hammer 配置文件中启用会话：

```
:foreman:
  :use_sessions: true
```

在 Hammer 中添加行强制使用会话。这意味着 Hammer 仅执行一次身份验证请求，而不是使用每个 hammer 命令。

2. 可选：通过将 :default_auth_type: 'Negotiate_Auth' 行添加到 foreman 参数，在 ~/.hammer/cli.modules.d/foreman.yml Hammer 配置文件中启用协商身份验证：

```
:foreman:
  :default_auth_type: 'Negotiate_Auth'
  :use_sessions: true
```

添加这一行意味着，当您进入第一个 hammer 命令时，会协商您的身份验证。如果存在此条目，Hammer 会尝试使用协商协议与 Satellite 服务器通信。

5.8. 置备的主机的外部身份验证

使用本节为 Red Hat Identity Management 域支持配置 Satellite 服务器或 Capsule 服务器，然后将主机添加到 Red Hat Identity Management 域组中。

先决条件

- 注册到 Content Delivery Network 或注册到 Satellite 服务器的外部胶囊服务器的 Satellite 服务器。
- 一个部署的领域或域提供商，如红帽身份管理。

在 Satellite 服务器或 Capsule 服务器上安装和配置红帽身份管理软件包：

要将 Red Hat Identity Management 用于置备的主机，请完成以下步骤在 Satellite 服务器或 Capsule 服务器上安装和配置 Red Hat Identity Management 软件包：

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

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

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

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

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

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

请注意返回和红帽身份管理服务器配置详情的主体名称，因为您需要以下步骤。

为 Red Hat Identity Management 域配置 Satellite 服务器或 Capsule 服务器支持：

在 Satellite 和您要使用的每个 Capsule 上完成以下步骤：

1. 将 /root/freeipa.keytab 文件复制到您要包含在同一主体和域中的任何 Capsule 服务器中：

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

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

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

3. 在您要包含在域中的所有 Capsule 上输入以下命令。如果您在 Satellite 上使用集成 Capsule，请在 Satellite 服务器上输入以下命令：

```
# satellite-installer --foreman-proxy-realm true \
--foreman-proxy-realm-keytab /etc/foreman-proxy/freeipa.keytab \
--foreman-proxy-realm-principal realm-capsule@EXAMPLE.COM \
```

```
--foreman-proxy-realm-provider freeipa
```

您也可以在首次配置 Satellite 服务器时使用这些选项。

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

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

5. 可选：如果您在现有 Satellite 服务器或 Capsule 服务器上配置 Red Hat Identity Management，请完成以下步骤以确保配置更改生效：

a. 重启 foreman-proxy 服务：

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

b. 在 Satellite Web UI 中，进入到 Infrastructure > Capsules。

c. 找到您为 Red Hat Identity Management 配置的 Capsule，然后从 Actions 列中的列表中，选择 Refresh。

为启用了 Red Hat Identity Management 的 Capsule 创建一个域

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

流程

1. 在 Satellite Web UI 中，进入到 Infrastructure > Realms 并点 Create Realm。

2. 在 Name 字段中输入域的名称。

3. 从 Realm Type 列表中，选择 realm 的类型。

4. 从 Realm Capsule 列表中，选择您配置 Red Hat Identity Management 的 Capsule 服务器。

5. 单击位置选项卡 并从 Locations 列表中选择您要添加新域的位置。

6. 单击 Organizations 选项卡并从 Organizations 列表中选择您要添加新域的组织。

7. 点 Submit。

使用域信息更新主机组

您必须更新要用于新域信息的任何主机组。

1. 在 Satellite Web UI 中，进入到 Configure > Host Groups，选择您要更新的主机组，然后点击 Network 选项卡。

2. 从 Realm 列表中，选择您创建的域作为此流程的一部分，然后单击 Submit。

将主机添加到红帽身份管理主机组

Red Hat Identity Management 支持根据系统的属性设置自动成员资格规则。Red Hat Satellite 的域功能使管理员能够将 Red Hat Satellite 主机组映射到红帽身份管理参数 userclass，供管理员配置自动成员。

使用嵌套的主机组时，它们会在 Red Hat Satellite 用户界面中显示时发送到红帽身份管理服务器。例如："Parent/Child/Child"。

Satellite 服务器或 Capsule 服务器向红帽身份管理服务器发送更新，但自动成员规则仅在初始注册时应用。

将主机添加到 Red Hat Identity Management 主机组：

1. 在 Red Hat Identity Management 服务器上，创建一个主机组：

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

2. 创建自动成员规则 ：

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

您可以使用以下选项：

- **automember-add** 将组标记为自动成员组。
- **--type=hostgroup** 标识目标组是主机组，而不是用户组。
- ***automember_rule*** 添加您要用来识别自动成员规则的名称。

3. 根据 **userclass** 属性定义自动成员条件：

```
# ipa automember-add-condition --key=userclass --type=hostgroup --inclusive-
regex=^webserver hostgroup_name
----------------------------------
Added condition(s) to "hostgroup_name"
----------------------------------
Automember Rule: automember_rule
Inclusive Regex: userclass=^webserver
----------------------------
Number of conditions added 1
----------------------------
```

您可以使用以下选项：

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

- *hostgroup_name* - 标识目标主机组的名称。

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

5.9. 使用红帽单点登录身份验证配置 SATELLITE

使用本节将 Satellite 配置为使用红帽单点登录作为外部身份验证的 OpenID 提供程序。

5.9.1. 使用红帽单点登录身份验证配置 Satellite 的先决条件

在使用 Red Hat Single Sign-On 外部身份验证配置 Satellite 前，请确保满足以下要求：

- 使用 HTTPS 而不是 HTTP 的 Red Hat Single Sign-On 服务器的工作安装。
- 具有 admin 权限的 Red Hat Single Sign-On 帐户。
- 在红帽单点登录中创建的 Satellite 用户帐户的域。
- 如果证书或 CA 是自签名的，请确保它们被添加到最终用户证书信任存储中。
- 导入或添加到 Red Hat Single Sign-On 的用户。

  如果您配置了现有用户数据库，如 LDAP 或 Kerberos，您可以通过配置用户联邦来从其中导入用户。如需更多信息，请参阅 *Red Hat Single Sign-On Server Administration Guide* 中的 User Storage Federation。

  如果您没有配置现有用户数据库，您可以在 Red Hat Single Sign-On 中手动创建用户。如需更多信息，请参阅 *红帽单点登录服务器管理指南中的创建新用户*。

5.9.2. 将 Satellite 注册为 Red Hat Single Sign-On 客户端

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

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

1. 用户使用 Satellite Web UI 向 Satellite 进行身份验证。

2. 用户使用 Satellite CLI 向 Satellite 进行身份验证。

您必须决定希望用户提前进行身份验证，因为这两种方法都需要将不同的 Satellite 客户端注册到 Red Hat Single Sign-On 并进行配置。在 Red Hat Single Sign-On 中注册和配置 Satellite 客户端的步骤在流程中区分。

如果要使用身份验证方法并相应地配置两个客户端，您还可以将两个不同的 Satellite 客户端注册到 Red Hat Single Sign-On。

流程

1. 在 Satellite 服务器中安装以下软件包：

```
# satellite-maintain packages install mod_auth_openidc keycloak-httpd-client-install python3-lxml
```

2. 将 Satellite 注册到 Red Hat Single Sign-On 作为客户端。请注意，您使用 Web UI 和 CLI 登录的注册过程会有所不同。您可以将两个客户端 Satellite 客户端注册到红帽单点登录，以便能够通过 Web UI 和 CLI 登录 Satellite。

   - 如果您希望用户使用 Web UI 向 Satellite 进行身份验证，请按如下所示创建一个客户端：

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

出现提示时，输入 管理帐户的密码。此命令在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

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

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

- 如果您希望用户使用 CLI 向 Satellite 进行身份验证，请按如下所示创建一个客户端：

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

出现提示时，输入 管理帐户的密码。此命令在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

3. 重启 httpd 服务：

```
# systemctl restart httpd
```

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

使用这个流程在 Red Hat Single Sign-On Web UI 中配置 Satellite 客户端，并为 Satellite 客户端创建组和受众映射程序。

流程

1. 在 Red Hat Single Sign-On Web UI 中，导航到 Clients 并单击 Satellite 客户端。
2. 配置访问类型：
   - 如果您希望用户使用 Satellite Web UI 向 Satellite 进行身份验证，请从 Access Type

列表中选择 **confidential**。

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

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

- 如果您希望用户使用 **Satellite Web UI** 向 **Satellite** 进行身份验证，请在现有 **URI** 下的空白字段中输入 **URI https://satellite.example.com/users/extlogin**。请注意，您必须在 **Satellite FQDN** 后添加字符串 **/users/extlogin**。

  完成此步骤后，使用 **Satellite Web UI** 登录的 **Satellite** 客户端必须具有以下 **Valid Redirect URI** ：

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

- 如果您希望用户使用 **CLI** 对 **Satellite** 进行身份验证，请在现有 **URI** 的空白字段中输入 **urn:ietf:wg:oauth:2.0:oob**。

  完成此步骤后，使用 **CLI** 登录的 **Satellite** 客户端必须具有以下 **Valid Redirect URI** ：

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

4. 点击 **Save**。

5. 点 **Mappers** 选项卡，然后点 **Create** 添加受众映射程序。

6. 在 **Name** 字段中输入 **audience mapper** 的名称。

7. 从 **Mapper Type** 列表中，选择 **Audience**。

8. 从 **Included Client Audience** 列表中，选择 **Satellite** 客户端。

9. 点击 **Save**。

10. 点 **Create** 添加组映射器，以便您可以根据组成员资格在 **Satellite** 中指定授权。

11. 在 **Name** 字段中输入组映射程序的名称。

12. 从 **Mapper Type** 列表中，选择 **Group Membership**。

13. 在 **Token Claim Name** 字段中输入组。

14. 将 **Full group path** 设置为 **OFF**。

15. 点击 **Save**。

5.9.4. 为红帽单点登录身份验证配置 Satellite 设置

使用本节通过 **Satellite Web UI** 或 **CLI** 为红帽单点登录身份验证配置 **Satellite**。

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

使用 **Satellite Web UI** 为 **Red Hat Single Sign-On** 身份验证配置 **Satellite** 设置。

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

先决条件

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

流程

1.

在 Satellite Web UI 中，进入到 Administer > Settings，然后点击 Authentication 选项卡。

2. 找到 Authorize login delegation 行，然后在 Value 列中将值设为 Yes。

3. 找到 Authorize login delegation auth source user autocreate 行，并在 Value 列中将值设为 External。

4. 找到 Login delegation logout URL 行，然后在 Value 列中将值设为 https://satellite.example.com/users/extlogout。

5. 找到 OIDC Algorithm 行，并在 Value 列中将 Red Hat Single Sign-On 上的编码的算法设置为 RS256。

6. 找到 OIDC Audience 行，并在 Value 列中为 Red Hat Single Sign-On 设置客户端 ID。

7. 找到 OIDC Issuer 行，并在 Value 列中将值设为 *https://RHSSO.example.com/auth/realms/Satellite_Realm*。

8. 找到 OIDC JWKs URL 行，并在 Value 列中将值设为 *https://RHSSO.example.com/auth/realms/Satellite_Realm/protocol/openid-connect/certs*。

9. 在 Satellite Web UI 中，进入到 Administer > Authentication Sources，点 External 卡中的垂直 ellipsis，然后选择 Edit。

10. 单击 Locations 选项卡，再添加可以使用 Red Hat Single Sign-On 身份验证源的位置。

11. 单击 Organizations 选项卡，再添加可以使用 Red Hat Single Sign-On 身份验证源的组织。

12. 点 Submit。

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

使用 Satellite CLI 为 Red Hat Single Sign-On 身份验证配置 Satellite 设置。

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

先决条件

- 确保 Red Hat Single Sign-On Web UI 中的 Satellite 客户端中的 Access Type 设置被设置为 public

流程

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

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

2. 设置登录委托注销 URL：

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

3. 在 Red Hat Single Sign-On 中设置编码的算法，例如 RS256 ：

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

4. 打开 *RHSSO.example.com*/auth/realms/*RHSSO_REALM*/.well-known/openid-configuration URL，并记下以下步骤中选项的值。

5. 在 Open IDC 受众中添加 Hammer 客户端的值：

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

注意

如果您将多个 Red Hat Single Sign-On 客户端注册到 Satellite，请确保将所有受众附加到阵列中。例如：

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

6. 为 Open IDC 签发者设置值：

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

7. 设置 Open IDC Java Web Token (JWT)的值：

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

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

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

9. 设置位置和机构：

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

5.9.5. 使用红帽单点登录登录到 Satellite Web UI

使用这个流程，使用红帽单点登录登录到 Satellite Web UI。

流程

- 在您的浏览器中，登录 Satellite 并输入您的凭据。

5.9.6. 使用红帽单点登录登录到 Satellite CLI

使用这个流程，使用代码授权类型向 Satellite CLI 进行身份验证。

流程

1. 要使用代码授权类型向 Satellite CLI 进行身份验证，请输入以下命令：

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

该命令会提示您输入一个成功的代码。

2. 若要检索成功代码，请导航到命令返回的 URL，并提供所需的信息。

3. 复制 Web UI 返回的成功代码。

4. 在 hammer auth 登录 oauth 的命令提示符中，输入用于向 Satellite CLI 进行身份验证的成功代码。

5.9.7. 为 Red Hat Single Sign-On 身份验证配置组映射

另外，为了实施基于角色的访问控制(RBAC)，请在 Satellite 中创建一个组，为该组分配一个角色，然后将 Active Directory 组映射到 Satellite 组。因此，Red Hat Single Sign-On 中给定组中的任何人都会在对应的 Satellite 组下登录。本例在 Active Directory 中配置 Satellite-admin 用户组的用户，以用户身份在 Satellite 上进行身份验证。

流程

1. 在 Satellite Web UI 中，进入到 Administer > User Groups。

2. 单击 Create User Group。

3. 在 Name 字段中输入用户组的名称。名称不应与 Active Directory 中的名称相同。

4. 不要将用户和用户组添加到右列中。点 Roles 选项卡。

5. 选中 Administer 复选框。

6. 点 External Groups 选项卡。

7. 单击 Add external user group。

8. 在 Name 字段中输入 Active Directory 组的名称。

9. 从列表中选择 EXTERNAL。

5.10. 使用 TOTP 配置 RED HAT SINGLE SIGN-ON 身份验证

使用本节将 Satellite 配置为使用红帽单点登录作为使用 TOTP 卡进行外部身份验证的 OpenID 提供程序。

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

在使用 Red Hat Single Sign-On 外部身份验证配置 Satellite 前，请确保满足以下要求：

- 使用 HTTPS 而不是 HTTP 的 Red Hat Single Sign-On 服务器的工作安装。
- 具有 admin 权限的 Red Hat Single Sign-On 帐户。
- 在红帽单点登录中创建的 Satellite 用户帐户的域。
- 如果证书或 CA 是自签名的，请确保它们被添加到最终用户证书信任存储中。

- 导入或添加到 Red Hat Single Sign-On 的用户。

如果您配置了现有用户数据库，如 LDAP 或 Kerberos，您可以通过配置用户联邦来从其中导入用户。如需更多信息，请参阅 *Red Hat Single Sign-On Server Administration Guide* 中的 User Storage Federation。

如果您没有配置现有用户数据库，您可以在 Red Hat Single Sign-On 中手动创建用户。如需更多信息，请参阅 *红帽单点登录服务器管理指南中的创建新用户*。

5.10.2. 将 Satellite 注册为 Red Hat Single Sign-On 客户端

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

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

1. 用户使用 Satellite Web UI 向 Satellite 进行身份验证。
2. 用户使用 Satellite CLI 向 Satellite 进行身份验证。

您必须决定希望用户提前进行身份验证，因为这两种方法都需要将不同的 Satellite 客户端注册到 Red Hat Single Sign-On 并进行配置。在 Red Hat Single Sign-On 中注册和配置 Satellite 客户端的步骤在流程中区分。

如果要使用身份验证方法并相应地配置两个客户端，您还可以将两个不同的 Satellite 客户端注册到 Red Hat Single Sign-On。

流程

1. 在 Satellite 服务器中安装以下软件包：

```
# satellite-maintain packages install mod_auth_openidc keycloak-httpd-client-install python3-lxml
```

2. 将 Satellite 注册到 Red Hat Single Sign-On 作为客户端。请注意，您使用 Web UI 和 CLI

登录的注册过程会有所不同。您可以将两个客户端 Satellite 客户端注册到红帽单点登录，以便能够通过 Web UI 和 CLI 登录 Satellite。

- 如果您希望用户使用 Web UI 向 Satellite 进行身份验证，请按如下所示创建一个客户端：

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

出现提示时，输入 管理帐户的密码。此命令在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

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

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

- 如果您希望用户使用 CLI 向 Satellite 进行身份验证，请按如下所示创建一个客户端：

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

出现提示时，输入 管理帐户的密码。此命令在 Red Hat Single Sign-On 中为 Satellite 创建客户端。

3. 重启 httpd 服务：

```
# systemctl restart httpd
```

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

使用这个流程在 Red Hat Single Sign-On Web UI 中配置 Satellite 客户端，并为 Satellite 客户端创建组和受众映射程序。

流程

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

     完成此步骤后，使用 Satellite Web UI 登录的 Satellite 客户端必须具有以下 Valid Redirect URI ：

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

   - 如果您希望用户使用 CLI 对 Satellite 进行身份验证，请在现有 URI 的空白字段中输入 urn:ietf:wg:oauth:2.0:oob。

     完成此步骤后，使用 CLI 登录的 Satellite 客户端必须具有以下 Valid Redirect URI ：

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

4. 点击 Save。

5. 点 Mappers 选项卡，然后点 Create 添加受众映射程序。

6. 在 Name 字段中输入 audience mapper 的名称。

7. 从 Mapper Type 列表中，选择 Audience。

8. 从 Included Client Audience 列表中，选择 Satellite 客户端。

9. 点击 Save。

10. 点 Create 添加组映射器，以便您可以根据组成员资格在 Satellite 中指定授权。

11. 在 Name 字段中输入组映射程序的名称。

12. 从 Mapper Type 列表中，选择 Group Membership。

13. 在 Token Claim Name 字段中输入组。

14. 将 Full group path 设置为 OFF。

15. 点击 Save。

5.10.4. 为红帽单点登录身份验证配置 Satellite 设置

使用本节通过 Satellite Web UI 或 CLI 为红帽单点登录身份验证配置 Satellite。

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

使用 Satellite Web UI 为 Red Hat Single Sign-On 身份验证配置 Satellite 设置。

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

先决条件

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

流程

1. 在 Satellite Web UI 中，进入到 Administer > Settings，然后点击 Authentication 选项卡。
2. 找到 Authorize login delegation 行，然后在 Value 列中将值设为 Yes。
3. 找到 Authorize login delegation auth source user autocreate 行，并在 Value 列中将值设为 External。
4. 找到 Login delegation logout URL 行，然后在 Value 列中将值设为 https://satellite.example.com/users/extlogout。
5. 找到 OIDC Algorithm 行，并在 Value 列中将 Red Hat Single Sign-On 上的编码的算法设置为 RS256。
6. 找到 OIDC Audience 行，并在 Value 列中为 Red Hat Single Sign-On 设置客户端 ID。
7. 找到 OIDC Issuer 行，并在 Value 列中将值设为 *https://RHSSO.example.com/auth/realms/Satellite_Realm*。
8. 找到 OIDC JWKs URL 行，并在 Value 列中将值设为 *https://RHSSO.example.com/auth/realms/Satellite_Realm/protocol/openid-connect/certs*。

9. 在 Satellite Web UI 中，进入到 Administer > Authentication Sources，点 External 卡中的垂直 ellipsis，然后选择 Edit。

10. 单击 Locations 选项卡，再添加可以使用 Red Hat Single Sign-On 身份验证源的位置。

11. 单击 Organizations 选项卡，再添加可以使用 Red Hat Single Sign-On 身份验证源的组织。

12. 点 Submit。

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

使用 Satellite CLI 为 Red Hat Single Sign-On 身份验证配置 Satellite 设置。

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

先决条件

- 确保 Red Hat Single Sign-On Web UI 中的 Satellite 客户端中的 Access Type 设置被设置为 public

流程

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

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

2. 设置登录委托注销 URL：

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

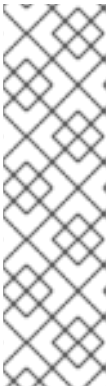
3. 在 Red Hat Single Sign-On 中设置编码的算法，例如 RS256 ：

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

4. **打开 *RHSSO.example.com*/auth/realms/*RHSSO_REALM*/.well-known/openid-configuration URL，并记下以下步骤中选项的值。**

5. **在 Open IDC 受众中添加 Hammer 客户端的值：**

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



注意

如果您将多个 Red Hat Single Sign-On 客户端注册到 Satellite，请确保将所有受众附加到阵列中。例如：

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

6. **为 Open IDC 签发者设置值：**

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

7. **设置 Open IDC Java Web Token (JWT)的值：**

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

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

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

9. **设置位置和机构：**

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

5.10.5. 使用 Red Hat Single Sign-On 配置 Satellite 进行 TOTP 身份验证

使用这个流程将 Satellite 配置为使用红帽单点登录作为带有基于时间的一次性密码(TOTP)的外部身份验证的 OpenID 提供程序。

流程

1. 在 Red Hat Single Sign-On Web UI 中，导航到 Satellite 域。
2. 导航到 Authentication，再单击 OTP Policy 选项卡。
3. 确保 支持的 Applications 字段包含 FreeOTP 或 Google Authenticator。
4. 配置 OTP 设置以满足您的要求。
5. 可选： 如果要使用 TOTP 身份验证作为所有用户的默认验证方法，点 Flows 选项卡，并在 OTP Form 设置右侧，选择 REQUIRED。
6. 点 Required Actions 选项卡。
7. 在 Configure OTP 行右侧，选中 Default Action 复选框。

5.10.6. 使用红帽单点登录 TOTP 身份验证登录到 Satellite Web UI

使用这个流程，使用 Red Hat Single Sign-On TOTP 身份验证登录到 Satellite Web UI。

流程

1. 登录 Satellite，Satellite 会将您重定向到 Red Hat Single Sign-On 登录屏幕。
2. 输入您的用户名和密码，然后点 Log In。
3. 第一次尝试登录，Red Hat Single Sign-On 请求您通过扫描 barcode 并输入显示的 pin 来

配置客户端。

4. 配置客户端并输入有效的 PIN 后，Red Hat Single Sign-On 会将您重定向到 Satellite 并登录您的日志。

5.10.7. 使用红帽单点登录登录到 Satellite CLI

使用这个流程，使用代码授权类型向 Satellite CLI 进行身份验证。

流程

1. 要使用代码授权类型向 Satellite CLI 进行身份验证，请输入以下命令：

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

该命令会提示您输入一个成功的代码。

2. 若要检索成功代码，请导航到命令返回的 URL，并提供所需的信息。

3. 复制 Web UI 返回的成功代码。

4. 在 hammer auth 登录 oauth 的命令提示符中，输入用于向 Satellite CLI 进行身份验证的成功代码。

5.10.8. 为 Red Hat Single Sign-On 身份验证配置组映射

另外，为了实施基于角色的访问控制(RBAC)，请在 Satellite 中创建一个组，为该组分配一个角色，然后将 Active Directory 组映射到 Satellite 组。因此，Red Hat Single Sign-On 中给定组中的任何人都会在对应的 Satellite 组下登录。本例在 Active Directory 中配置 Satellite-admin 用户组的用户，以用户身份在 Satellite 上进行身份验证。

流程

1. 在 Satellite Web UI 中，进入到 Administer > User Groups。
2. 单击 Create User Group。
3. 在 Name 字段中输入用户组的名称。名称不应与 Active Directory 中的名称相同。
4. 不要将用户和用户组添加到右列中。点 Roles 选项卡。
5. 选中 Administer 复选框。
6. 点 External Groups 选项卡。
7. 单击 Add external user group。
8. 在 Name 字段中输入 Active Directory 组的名称。
9. 从列表中选择 EXTERNAL。

5.11. 禁用 RED HAT SINGLE SIGN-ON 身份验证

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

流程

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

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

第 6 章 使用外部服务配置 SATELLITE 服务器

如果您不想在 Satellite 服务器上配置 DNS、DHCP 和 TFTP 服务，请使用本节将 Satellite 服务器配置为处理外部 DNS、DHCP 和 TFTP 服务。

6.1. 使用外部 DNS 配置 SATELLITE 服务器

您可以使用外部 DNS 配置 Satellite 服务器。Satellite 服务器使用 nsupdate 实用程序更新远程服务器上的 DNS 记录。

要使任何更改持久，您必须使用适合您的环境的选项输入 satellite-installer 命令。

先决条件

- 您必须已配置了外部 DNS 服务器。
- 本指南假设您有现有的安装。

流程

1. 将 /etc/rndc.key 文件从外部 DNS 服务器复制到 Satellite 服务器：

```
# scp root@dns.example.com:/etc/rndc.key /etc/foreman-proxy/rndc.key
```

2. 配置所有权、权限和 SELinux 上下文：

```
# restorecon -v /etc/foreman-proxy/rndc.key
# chown -v root:foreman-proxy /etc/foreman-proxy/rndc.key
# chmod -v 640 /etc/foreman-proxy/rndc.key
```

3. 要测试 nsupdate 工具，请远程添加主机：

```
# echo -e "server DNS_IP_Address\n \
update add aaa.example.com 3600 IN A Host_IP_Address\n \
send\n" | nsupdate -k /etc/foreman-proxy/rndc.key
# nslookup aaa.example.com DNS_IP_Address
```

```
# echo -e "server DNS_IP_Address\n \
update delete aaa.example.com 3600 IN A Host_IP_Address\n \
send\n" | nsupdate -k /etc/foreman-proxy/rndc.key
```

4. **输入 satellite-installer 命令，对 /etc/foreman-proxy/settings.d/dns.yml 文件进行以下更改：**

```
# satellite-installer --foreman-proxy-dns=true \
--foreman-proxy-dns-managed=false \
--foreman-proxy-dns-provider=nsupdate \
--foreman-proxy-dns-server="DNS_IP_Address" \
--foreman-proxy-keyfile=/etc/foreman-proxy/rndc.key
```

5. **在 Satellite Web UI 中，进入到 Infrastructure > Capsules。**

6. **找到 Satellite Server，然后从 Actions 列中的列表中选择 Refresh。**

7. **将 DNS 服务与适当的子网和域关联。**

6.2. 使用外部 DHCP 配置 SATELLITE 服务器

要使用外部 DHCP 配置 Satellite 服务器，您必须完成以下步骤：

1. **第 6.2.1 节 “配置外部 DHCP 服务器以用于 Satellite 服务器”**

2. **第 6.2.2 节 “使用外部 DHCP 服务器配置 Satellite 服务器”**

6.2.1. 配置外部 DHCP 服务器以用于 Satellite 服务器

要将运行 Red Hat Enterprise Linux 的外部 DHCP 服务器配置为与 Satellite 服务器搭配使用，您必须安装 ISC DHCP Service 和 Berkeley Internet Name Domain (BIND)工具软件包。您还必须与 Satellite 服务器共享 DHCP 配置和租用文件。此流程中的示例使用分布式网络文件系统(NFS)协议共享 DHCP 配置和租期文件。

注意

如果您使用 dnsmasq 作为外部 DHCP 服务器，请启用 dhcp-no-override 设置。这是必要的，因为 Satellite 在 TFTP 服务器上创建 grub2/ 子目录下的配置文件。如果禁用 dhcp-no-override 设置，主机会从根目录获取引导装载程序及其配置，这可能会导致错误。

流程

1. **在 Red Hat Enterprise Linux 主机上，安装 ISC DHCP 服务和 Berkeley Internet Name Domain (BIND)工具软件包：**

```
# dnf install dhcp-server bind-utils
```

2. **生成安全令牌：**

```
# dnssec-keygen -a HMAC-MD5 -b 512 -n HOST omapi_key
```

因此，当前目录中创建由两个文件组成的密钥对。

3. **从密钥复制 secret 哈希：**

```
# grep ^Key Komapi_key.+*.private | cut -d ' ' -f2
```

4. **编辑所有子网的 dhcpd 配置文件并添加密钥。以下是一个示例：**

```
# cat /etc/dhcp/dhcpd.conf
default-lease-time 604800;
max-lease-time 2592000;
log-facility local7;

subnet 192.168.38.0 netmask 255.255.255.0 {
 range 192.168.38.10 192.168.38.100;
 option routers 192.168.38.1;
 option subnet-mask 255.255.255.0;
 option domain-search "virtual.lan";
 option domain-name "virtual.lan";
 option domain-name-servers 8.8.8.8;
}

omapi-port 7911;
key omapi_key {
 algorithm HMAC-MD5;
```

```
 secret "My_Secret";
};
omapi-key omapi_key;
```

请注意，选项 **router** 值是您要与外部 **DHCP** 服务一起使用的 **Satellite** 服务器或 **Capsule** 服务器的 **IP** 地址。

5. 从在其中创建文件的目录中删除这两个密钥文件。

6. 在管理门户中，定义每个子网。不要为定义的子网设置 **DHCP Capsule**。

要防止冲突，请单独设置租期和保留范围。例如，如果租期范围是 **192.168.38.10** 到 **192.168.38.100**，在 **Satellite Web UI** 中将保留范围定义为 **192.168.38.101 to 192.168.38.250**。

7. 配置防火墙以从外部访问 **DHCP** 服务器：

```
# firewall-cmd --add-service dhcp
```

8. 使更改持久：

```
# firewall-cmd --runtime-to-permanent
```

9. 在 **Satellite** 服务器上，确定 **foreman** 用户的 **UID** 和 **GID**：

```
# id -u foreman
993
# id -g foreman
990
```

10. 在 **DHCP** 服务器上，创建 **foreman** 用户和组，其 **ID** 与上一步中确定的 **ID** 相同：

```
# groupadd -g 990 foreman
# useradd -u 993 -g 990 -s /sbin/nologin foreman
```

11. 要确保配置文件可以访问，请恢复读取和执行标记：

```
# chmod o+rx /etc/dhcp/
# chmod o+r /etc/dhcp/dhcpd.conf
# chattr +i /etc/dhcp/ /etc/dhcp/dhcpd.conf
```

12. **启用并启动 DHCP 服务：**

```
# systemctl enable --now dhcpd
```

13. **使用 NFS 导出 DHCP 配置和租期文件：**

```
# dnf install nfs-utils
# systemctl enable --now nfs-server
```

14. **为您要使用 NFS 导出的 DHCP 配置和租期文件创建目录：**

```
# mkdir -p /exports/var/lib/dhcpd /exports/etc/dhcp
```

15. **要为创建的目录创建挂载点，请在 /etc/fstab 文件中添加以下行：**

```
/var/lib/dhcpd /exports/var/lib/dhcpd none bind,auto 0 0
/etc/dhcp /exports/etc/dhcp none bind,auto 0 0
```

16. **在 /etc/fstab 中挂载文件系统：**

```
# mount -a
```

17. **确保 /etc/exports 中存在以下行：**

```
/exports 192.168.38.1(rw,async,no_root_squash,fsid=0,no_subtree_check)

/exports/etc/dhcp 192.168.38.1(ro,async,no_root_squash,no_subtree_check,nohide)

/exports/var/lib/dhcpd 192.168.38.1(ro,async,no_root_squash,no_subtree_check,nohide)
```

请注意，您输入的 IP 地址是您要与外部 DHCP 服务一起使用的 Satellite 或 Capsule IP 地址。

18. 重新载入 NFS 服务器：

```
# exportfs -rva
```

19. 为 DHCP omapi 端口 7911 配置防火墙：

```
# firewall-cmd --add-port=7911/tcp
```

20. 可选：配置防火墙以从外部访问 NFS。客户端使用 NFSv3 配置。

```
# firewall-cmd \
--add-service mountd \
--add-service nfs \
--add-service rpc-bind \
--zone public
```

21. 使更改持久：

```
# firewall-cmd --runtime-to-permanent
```

6.2.2. 使用外部 DHCP 服务器配置 Satellite 服务器

您可以使用外部 DHCP 服务器配置 Satellite 服务器。

先决条件

- 确保您已配置了外部 DHCP 服务器，并且您已与 Satellite 服务器共享 DHCP 配置和租用文件。更多信息请参阅 第 6.2.1 节 “配置外部 DHCP 服务器以用于 Satellite 服务器”。

流程

1. 安装 nfs-utils 软件包：

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

2. 为 NFS 创建 DHCP 目录：

```
# mkdir -p /mnt/nfs/etc/dhcp /mnt/nfs/var/lib/dhcpd
```

3. **更改文件所有者：**

```
# chown -R foreman-proxy /mnt/nfs
```

4. **验证与 NFS 服务器和远程过程调用(RPC)通信路径的通信：**

```
# showmount -e DHCP_Server_FQDN
# rpcinfo -p DHCP_Server_FQDN
```

5. **在 /etc/fstab 文件中添加以下行：**

```
DHCP_Server_FQDN:/exports/etc/dhcp /mnt/nfs/etc/dhcp nfs
ro,vers=3,auto,nosharecache,context="system_u:object_r:dhcp_etc_t:s0" 0 0

DHCP_Server_FQDN:/exports/var/lib/dhcpd /mnt/nfs/var/lib/dhcpd nfs
ro,vers=3,auto,nosharecache,context="system_u:object_r:dhcpd_state_t:s0" 0 0
```

6. **在 /etc/fstab 中挂载文件系统：**

```
# mount -a
```

7. **要验证 foreman-proxy 用户可以访问通过网络共享的文件，请显示 DHCP 配置和租期文件：**

```
# su foreman-proxy -s /bin/bash
$ cat /mnt/nfs/etc/dhcp/dhcpd.conf
$ cat /mnt/nfs/var/lib/dhcpd/dhcpd.leases
$ exit
```

8. **输入 satellite-installer 命令，对 /etc/foreman-proxy/settings.d/dhcp.yml 文件进行以下更改：**

```
# satellite-installer \
--enable-foreman-proxy-plugin-dhcp-remote-isc \
--foreman-proxy-dhcp-provider=remote_isc \
--foreman-proxy-dhcp-server=My_DHCP_Server_FQDN \
--foreman-proxy-dhcp=true \
--foreman-proxy-plugin-dhcp-remote-isc-dhcp-config /mnt/nfs/etc/dhcp/dhcpd.conf \
--foreman-proxy-plugin-dhcp-remote-isc-dhcp-leases /mnt/nfs/var/lib/dhcpd/dhcpd.leases \
```

```
--foreman-proxy-plugin-dhcp-remote-isc-key-name=omapi_key \
--foreman-proxy-plugin-dhcp-remote-isc-key-secret=My_Secret \
--foreman-proxy-plugin-dhcp-remote-isc-omapi-port=7911
```

9. **将 DHCP 服务与适当的子网和域关联。**

6.3. 使用外部 TFTP 配置 SATELLITE 服务器

您可以使用外部 TFTP 服务配置 Satellite 服务器。

流程

1. 为 **NFS 创建 TFTP 目录：**

```
# mkdir -p /mnt/nfs/var/lib/tftpboot
```

2. **在 /etc/fstab 文件中，添加以下行：**

```
TFTP_Server_IP_Address:/exports/var/lib/tftpboot /mnt/nfs/var/lib/tftpboot nfs
rw,vers=3,auto,nosharecache,context="system_u:object_r:tftpdir_rw_t:s0" 0 0
```

3. **在 /etc/fstab 中挂载文件系统：**

```
# mount -a
```

4. **输入 satellite-installer 命令，对 /etc/foreman-proxy/settings.d/tftp.yml 文件进行以下更改：**

```
# satellite-installer \
--foreman-proxy-tftp-root /mnt/nfs/var/lib/tftpboot \
--foreman-proxy-tftp=true
```

5. **如果 TFTP 服务在与 DHCP 服务不同的服务器上运行，请使用 TFTP 服务运行的服务器的 FQDN 或 IP 地址更新 tftp_servername 设置：**

```
# satellite-installer --foreman-proxy-tftp-servername=TFTP_Server_FQDN
```

6. 在 Satellite Web UI 中，进入到 Infrastructure > Capsules。

7. 找到 Satellite Server，然后从 Actions 列中的列表中选择 Refresh。

8. 将 TFTP 服务与适当的子网和域关联。

6.4. 使用外部 IDM DNS 配置 SATELLITE 服务器

当 Satellite 服务器为主机添加 DNS 记录时，它会首先确定哪个胶囊为该域提供 DNS。然后，它与配置为为您的部署提供 DNS 服务的 Capsule 通信并添加记录。主机不涉及此过程。因此，您必须在当前配置为使用 IdM 服务器管理的域提供 DNS 服务的 Satellite 或 Capsule 上安装和配置 IdM 客户端。

Satellite 服务器可以配置为使用红帽身份管理(IdM)服务器来提供 DNS 服务。有关红帽身份管理的更多信息，请参阅 Linux 域身份、身份验证和策略指南。

要将 Satellite 服务器配置为使用 Red Hat Identity Management (IdM)服务器来提供 DNS 服务，请使用以下流程之一：

- 第 6.4.1 节 “使用 GSS-TSIG 身份验证配置动态 DNS 更新”
- 第 6.4.2 节 “使用 TSIG 身份验证配置动态 DNS 更新”

要恢复到内部 DNS 服务，请使用以下流程：

- 第 6.4.3 节 “恢复到内部 DNS 服务”

注意

您不需要使用 Satellite 服务器来管理 DNS。当您使用 Satellite 的域注册功能时，调配的主机会自动注册到 IdM 时，ipa-client-install 脚本会为客户端创建 DNS 记录。使用外部 IdM DNS 和域注册配置 Satellite 服务器是互斥的。有关配置域注册的详情，请参考第 5.8 节 “置备的主机的外部身份验证”。

6.4.1. 使用 GSS-TSIG 身份验证配置动态 DNS 更新

您可以将 IdM 服务器配置为对 RFC3645 中定义的 secret 密钥事务(GSS-TSIG)技术使用通用安全服务算法。要将 IdM 服务器配置为使用 GSS-TSIG 技术，您必须在 Satellite 服务器基本操作系统上安装 IdM 客户端。

先决条件

- 您必须确保 IdM 服务器已部署，并且基于主机的防火墙已正确配置。如需更多信息，请参阅 *安装身份管理指南* 中的 IdM 的端口要求。
- 您必须联系 IdM 服务器管理员，以确保在 IdM 服务器上获取具有在 IdM 服务器上创建区域权限的 IdM 服务器上的帐户。
- 您应创建应答文件的备份。如果应答文件损坏，您可以使用备份将应答文件恢复到其原始状态。如需更多信息，请参阅配置 Satellite 服务器。

流程

要使用 GSS-TSIG 身份验证配置动态 DNS 更新，请完成以下步骤：

在 IdM 服务器中创建 Kerberos 主体

1. 为从 IdM 管理员获取的帐户获取 Kerberos 票据：

```
# kinit idm_user
```

2. 为 Satellite 服务器创建一个新的 Kerberos 主体，用于在 IdM 服务器上进行身份验证：

```
# ipa service-add capsule/satellite.example.com
```

安装和配置 idM 客户端

1. 在为部署管理 DNS 服务的 Satellite 或 Capsule 的基本操作系统中，安装 ipa-client 软件包：

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

2. 运行安装脚本并根据屏幕提示配置 IdM 客户端：

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

3. 获取Kerberos ticket：

```
# kinit admin
```

4. 删除任何已存在的 keytab ：

```
# rm /etc/foreman-proxy/dns.keytab
```

5. 获取这个系统的 keytab ：

```
# ipa-getkeytab -p capsule/satellite.example.com@EXAMPLE.COM \
-s idm1.example.com -k /etc/foreman-proxy/dns.keytab
```

注意

将 keytab 添加到与服务中原始系统相同的备用系统时，添加 r 选项以防止生成新凭证并在原始系统上渲染凭证无效。

6. 对于 dns.keytab 文件，将 group 和 owner 设置为 foreman-proxy ：

```
# chown foreman-proxy:foreman-proxy /etc/foreman-proxy/dns.keytab
```

7. 可选： 要验证 keytab 文件是否有效，请输入以下命令：

```
# kinit -kt /etc/foreman-proxy/dns.keytab \
capsule/satellite.example.com@EXAMPLE.COM
```

在 IdM Web UI 中配置 DNS 区域

1. 创建并配置您要管理的区域：

a. 导航到 **Network Services > DNS > DNS Zones**。

b. 选择 **Add** 并输入区域名称。例如： **example.com**。

c. 点 **Add and Edit**。

d. 点 **Settings** 选项卡并在 **BIND 更新策略** 框中，将以下内容添加到分号分隔列表中：

```
grant capsule\047satellite.example.com@EXAMPLE.COM wildcard * ANY;
```

e. 将 **Dynamic update** 设置为 **True**。

f. 启用 **Allow PTR** 同步。

g. 点 **Save** 保存更改。

2. 创建并配置反向区：

a. 导航到 **Network Services > DNS > DNS Zones**。

b. 点击 **Add**。

c. 选择 **Reverse zone IP** 网络，并以 **CIDR** 格式添加网络地址以启用反向查找。

d. 点 **Add and Edit**。

e. 点 **Settings** 选项卡并在 **BIND 更新策略** 框中，将以下内容添加到分号分隔列表中：

```
grant capsule\047satellite.example.com@EXAMPLE.COM wildcard * ANY;
```

f. 将 **Dynamic update** 设置为 **True**。

g. 点 **Save** 保存更改。

配置管理域的 DNS 服务的 Satellite 或 Capsule 服务器

1. 使用 **satellite-installer** 命令配置管理域的 DNS 服务的 Satellite 或 Capsule：

- 在 **Satellite** 上输入以下命令：

```
# satellite-installer --scenario satellite \
--foreman-proxy-dns-managed=false \
--foreman-proxy-dns-provider=nsupdate_gss \
--foreman-proxy-dns-server="idm1.example.com" \
--foreman-proxy-dns-tsig-keytab=/etc/foreman-proxy/dns.keytab \
--foreman-proxy-dns-tsig-principal="capsule/satellite.example.com@EXAMPLE.COM" \
--foreman-proxy-dns=true
```

- 在 **Capsule** 上输入以下命令：

```
# satellite-installer --scenario capsule \
--foreman-proxy-dns-managed=false \
--foreman-proxy-dns-provider=nsupdate_gss \
--foreman-proxy-dns-server="idm1.example.com" \
--foreman-proxy-dns-tsig-keytab=/etc/foreman-proxy/dns.keytab \
--foreman-proxy-dns-tsig-principal="capsule/satellite.example.com@EXAMPLE.COM" \
--foreman-proxy-dns=true
```

运行 **satellite-installer** 命令并对 **Capsule** 配置进行任何更改后，您必须更新 **Satellite Web UI** 中每个受影响的胶囊的配置。

在 Satellite Web UI 中更新配置

1. 在 **Satellite Web UI** 中，进入到 **Infrastructure > Capsules**，找到 **Satellite** 服务器，从 **Actions** 列中的列表中，选择 **Refresh**。

2. 配置域：

a. 在 Satellite Web UI 中，进入到 Infrastructure > Domains 并选择域名。

b. 在 Domain 选项卡中，确保 DNS Capsule 设置为连接子网的胶囊。

3. 配置子网：

a. 在 Satellite Web UI 中，进入到 Infrastructure > Subnets 并选择子网名称。

b. 在 Subnet 选项卡中，将 IPAM 设置为 None。

c. 在 Domains 选项卡中，选择您要使用 IdM 服务器管理的域。

d. 在 Capsules 选项卡中，确保 Reverse DNS Capsule 设置为连接子网的 Capsule。

e. 点 Submit 以保存更改。

6.4.2. 使用 TSIG 身份验证配置动态 DNS 更新

您可以将 IdM 服务器配置为对 DNS (TSIG)技术使用 rndc.key 密钥文件进行身份验证的 secret 密钥事务身份验证。TSIG 协议在 RFC2845 中定义。

先决条件

- 您必须确保 IdM 服务器已部署，并且基于主机的防火墙已正确配置。如需更多信息，请参阅 *Linux 域身份、身份验证和策略指南* 中的 端口要求。
- 您必须在 IdM 服务器上获取 root 用户访问权限。
- 您必须确认 Satellite 服务器或 Capsule 服务器是否已配置为为您的部署提供 DNS 服务。
- 您必须在为部署管理 DNS 服务的 Satellite 或 Capsule 的基本操作系统上配置 DNS、DHCP

和 TFTP 服务。

- 您必须创建应答文件的备份。如果应答文件损坏，您可以使用备份将应答文件恢复到其原始状态。如需更多信息，请参阅配置 Satellite 服务器。

流程

要使用 TSIG 身份验证配置动态 DNS 更新，请完成以下步骤：

在 IdM 服务器中启用对 DNS 区的外部更新

1. 在 IdM 服务器上，将以下内容添加到 /etc/named.conf 文件的顶部：

```
############################################################################

include "/etc/rndc.key";
controls  {
inet _IdM_Server_IP_Address_ port 953 allow { _Satellite_IP_Address_; } keys { "rndc-key";
};
};
############################################################################
```

2. 重新载入 named 服务以使更改生效：

```
# systemctl reload named
```

3. 在 IdM Web UI 中，进入到 Network Services & gt; DNS > DNS Zones 并点区的名称。在 Settings 选项卡中，应用以下更改：

   a. 在 BIND 更新策略框中添加以下内容 ：

   ```
   grant "rndc-key" zonesub ANY;
   ```

   b. 将 Dynamic update 设置为 True。

   c. 点 Update 保存更改。

4.

将 /etc/rndc.key 文件从 IdM 服务器复制到 Satellite 服务器的基本操作系统。使用以下命令：

```
# scp /etc/rndc.key root@satellite.example.com:/etc/rndc.key
```

5. 要为 rndc.key 文件设置正确的所有权、权限和 SELinux 上下文，请输入以下命令：

```
# restorecon -v /etc/rndc.key
# chown -v root:named /etc/rndc.key
# chmod -v 640 /etc/rndc.key
```

6. 手动将 foreman-proxy 用户分配给 named 组。通常，satellite-installer 确保 foreman-proxy 用户属于 named UNIX 组，但是在这种情况下，Satellite 不管理用户和组，因此您需要手动将 foreman-proxy 用户分配给 named 组。

```
# usermod -a -G named foreman-proxy
```

7. 在 Satellite 服务器上，输入以下 satellite-installer 命令，将 Satellite 配置为使用外部 DNS 服务器：

```
# satellite-installer --scenario satellite \
--foreman-proxy-dns-managed=false \
--foreman-proxy-dns-provider=nsupdate \
--foreman-proxy-dns-server="IdM_Server_IP_Address" \
--foreman-proxy-dns-ttl=86400 \
--foreman-proxy-dns=true \
--foreman-proxy-keyfile=/etc/rndc.key
```

测试 IdM 服务器中的 DNS 区的外部更新

1. 确保 Satellite 服务器上的 /etc/rndc.key 文件中的密钥与 IdM 服务器上使用的密钥相同：

```
key "rndc-key" {
        algorithm hmac-md5;
        secret "secret-key==";
};
```

2. 在受管主机上，为主机创建测试 DNS 条目。例如，主机 *test.example.com* 在 IdM 服务器上 A 记录为 192.168.25.20，地址为 192.168.25.1。

```
# echo -e "server 192.168.25.1\n \
update add test.example.com 3600 IN A 192.168.25.20\n \
send\n" | nsupdate -k /etc/rndc.key
```

3. 在 Satellite 服务器上，测试 DNS 条目：

```
# nslookup test.example.com 192.168.25.1
Server:  192.168.25.1
Address: 192.168.25.1#53

Name: test.example.com
Address: 192.168.25.20
```

4. 要在 IdM web UI 中查看条目，请进入 Network Services > DNS > DNS Zones。单击区域的名称，再按名称搜索主机。

5. 如果成功解析，请删除测试 DNS 条目：

```
# echo -e "server 192.168.25.1\n \
update delete test.example.com 3600 IN A 192.168.25.20\n \
send\n" | nsupdate -k /etc/rndc.key
```

6. 确认 DNS 条目已被删除：

```
# nslookup test.example.com 192.168.25.1
```

以上 nslookup 命令失败，如果记录被成功删除，则返回 SERVFAIL 错误消息。

6.4.3. 恢复到内部 DNS 服务

您可以恢复到使用 Satellite 服务器和 Capsule 服务器作为 DNS 提供程序。您可以使用配置外部 DNS 之前创建的应答文件备份，或者您可以创建应答文件的备份。有关应答文件的更多信息，请参阅配置 Satellite 服务器。

流程

在您要配置为管理域的 DNS 服务的 Satellite 或 Capsule 服务器上，完成以下步骤：

将 Satellite 或 Capsule 配置为 DNS 服务器

- 如果您在配置外部 DNS 前创建了回答文件备份，请恢复应答文件，然后输入 satellite-installer 命令：

```
# satellite-installer
```

- 如果您没有应答文件的合适的备份，请立即创建应答文件的备份。要在不使用应答文件的情况下将 Satellite 或 Capsule 配置为 DNS 服务器，请在 Satellite 或 Capsule 上输入以下 satellite-installer 命令：

```
# satellite-installer \
--foreman-proxy-dns-managed=true \
--foreman-proxy-dns-provider=nsupdate \
--foreman-proxy-dns-server="127.0.0.1" \
--foreman-proxy-dns=true
```

如需更多信息，请参阅 在胶囊服务器上配置 DNS、DHCP 和 TFTP。

运行 satellite-installer 命令并对 Capsule 配置进行任何更改后，您必须更新 Satellite Web UI 中每个受影响的胶囊的配置。

在 Satellite Web UI 中更新配置

1. 在 Satellite Web UI 中，进入到 Infrastructure > Capsules。
2. 对于您要更新的每个胶囊，从 Actions 列表中选择 Refresh。
3. 配置域：
   a. 在 Satellite Web UI 中，进入到 Infrastructure > Domains，然后点击您要配置的域名。
   b. 在 Domain 选项卡中，将 DNS Capsule 设置为连接子网的胶囊。
4. 配置子网：
   a. 在 Satellite Web UI 中，进入到 Infrastructure > Subnets 并选择子网名称。

.

b. **在 Subnet 选项卡中，将 IPAM 设置为 DHCP 或 Internal DB。**

c. **在 Domains 选项卡中，选择您要使用 Satellite 或 Capsule 管理的域。**

d. **在 Capsules 选项卡中，将 Reverse DNS Capsule 设置为连接子网的胶囊。**

e. **点 Submit 以保存更改。**

附录 A. DNF 模块故障排除

如果 DNF 模块无法启用，这可能代表启用了不正确的模块。在这种情况下，您必须手动解析依赖项，如下所示。列出启用的模块：

```
# dnf module list --enabled
```

A.1. RUBY

如果 Ruby 模块无法启用，这可能代表启用了不正确的模块。在这种情况下，您必须手动解析依赖项，如下所示：

列出启用的模块：

```
# dnf module list --enabled
```

如果启用了 Ruby 2.5 模块，请执行模块重置：

```
# dnf module reset ruby
```

A.2. POSTGRESQL

如果 PostgreSQL 模块无法启用，这可能意味着启用了不正确的模块。在这种情况下，您必须手动解析依赖项，如下所示：

列出启用的模块：

```
# dnf module list --enabled
```

如果启用了 PostgreSQL 10 模块，请执行模块重置：

```
# dnf module reset postgresql
```

如果数据库之前使用 PostgreSQL 10 创建，请执行升级：

1. **启用 DNF 模块：**

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

2. **安装 PostgreSQL 升级软件包：**

```
# dnf install postgresql-upgrade
```

3. **执行升级：**

```
# postgresql-setup --upgrade
```

附录 B. 将自定义配置应用到 RED HAT SATELLITE

当您使用 satellite-installer 首次安装和配置 Satellite 时，您可以指定 DNS 和 DHCP 配置文件不由 Puppet 使用安装程序标志 --foreman-proxy-dns-managed=false 和 --foreman-proxy-dhcp-managed=false 管理。如果在初始安装程序运行期间没有指定这些标志，则重新运行安装程序会覆盖所有手动更改，例如，用于升级目的。如果更改被覆盖，您必须运行恢复过程来恢复手动更改。如需更多信息，请参阅恢复由 Puppet 运行编写的手动更改。

要查看所有可用于自定义配置的安装程序标志，请运行 satellite-installer --scenario satellite --full-help。有些 Puppet 类不公开给卫星安装程序。要手动管理它们并防止安装程序覆盖其值，请通过向配置文件 /etc/foreman-installer/custom-hiera.yaml 添加条目来指定配置值。此配置文件采用 YAML 格式，每行包含一个条目，格式为 < puppet class>::<parameter name>: <value>。此文件中指定的配置值会在安装程序重新运行后保留。

常见示例包括：

- 对于 Apache，将 ServerTokens 指令设置为仅返回产品名称：

```
apache::server_tokens: Prod
```

- 完全关闭 Apache 服务器签名：

```
apache::server_signature: Off
```

Satellite 安装程序的 Puppet 模块存储在 /usr/share/foreman-installer/modules 下。检查 .pp 文件（例如： *moduleName*/manifests/*example*.pp）来查找类、参数和值。或者，使用 grep 命令进行关键字搜索。

设置一些值可能会对 Red Hat Satellite 的性能或功能造成意外的后果。在应用之前，请考虑更改的影响，然后首先测试非生产环境中的更改。如果您没有非生产环境的 Satellite 环境，请使用 --noop 和 --verbose 选项运行 Satellite 安装程序。如果更改造成问题，请从 custom-hiera.yaml 中删除关闭行，然后重新运行 Satellite 安装程序。如果您对特定值是否安全改变，请联络红帽支持。

附录 C. 恢复 PUPPET 运行覆盖的手动更改

如果您的手动配置已被 Puppet 运行覆盖，您可以将文件恢复到之前的状态。下例演示了如何恢复由 Puppet 运行覆盖的 DHCP 配置文件。

流程

1. 复制您要恢复的文件。这可让您比较文件来检查升级所需的任何强制更改。对于 DNS 或 DHCP 服务，这并不常见。

```
# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.backup
```

2. 检查日志文件，以记下覆盖文件的 md5sum。例如：

```
# journalctl -xe
...
/Stage[main]/Dhcp/File[/etc/dhcp/dhcpd.conf]: Filebucketed /etc/dhcp/dhcpd.conf to puppet
with sum 622d9820b8e764ab124367c68f5fa3a1
...
```

3. 恢复覆盖的文件：

```
# puppet filebucket restore --local --bucket \
/var/lib/puppet/clientbucket /etc/dhcp/dhcpd.conf \ 622d9820b8e764ab124367c68f5fa3a1
```

4. 比较备份文件和恢复的文件，并编辑恢复的文件，使其包含升级所需的任何强制更改。