Red Hat Satellite 6.10

从连接的网络安装 Satellite 服务器

从连接的网络安装 Red Hat Satellite Server

Last Updated: 2024-01-31

Red Hat Satellite 6.10 从连接的网络安装 Satellite 服务器

从连接的网络安装 Red Hat Satellite Server

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，执行初始配置并配置外部服务。

目录

第 1 章 为安装准备您的环境

在安装 Satellite 之前，请确保您的环境满足以下要求。

1.1. 系统要求

以下要求适用于网络的基本操作系统：

- x86_64 架构
- 最新版本的 Red Hat Enterprise Linux 7 Server
- 至少 4 核 2.0 GHz CPU
- 卫星服务器需要至少 20 GB RAM 才能正常工作。另外，我们推荐至少具有 4 GB 交换空间的 RAM。以 RAM 低于最小值运行的卫星可能无法正确运行。
- 唯一主机名，可以包含小写字母、数字、点(.)和连字符(-)
- 当前的 Red Hat Satellite 订阅
- 管理用户(root)访问权限
- 系统 umask 为 0022
- 使用完全限定域名进行完整正向和反向 DNS 解析

卫星仅支持 **UTF-8** 编码。如果您的地区是美国且您的语言为英文，请将 **en_US.utf-8** 设置为系统范围区域设置。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。在安装卫星服务器前，请确保您的环境满足安装要求。

除了运行卫星服务器外，必须在全新调配的系统上安装卫星服务器，从而不提供其他功能。全新调配的系统不得具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
- puppetserver
- qdrouterd
- qpidd
- redis
- tomcat

认证的虚拟机监控程序

在支持运行 Red Hat Enterprise Linux 的 hypervisor 上运行的物理系统和虚拟机上都完全支持卫星服务器。有关认证的虚拟机监控程序的更多信息，请参阅 哪些管理程序已经认证可运行 Red Hat Enterprise Linux？

SELinux Mode

必须启用 SELinux，无论是 enforcing 模式还是 permissive 模式。不支持使用禁用 SELinux 的安装。

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 *Red Hat Enterprise Linux Security Guide* 中启用 FIPS 模式。

1.2. 存储要求

- Red Hat Enterprise Linux 7

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。

运行时大小通过 Red Hat Enterprise Linux 6、7 和 8 软件仓库同步进行测量。

1.2.1. Red Hat Enterprise Linux 7

表 1.1. 卫星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/opt/rh/rh-postgresql12/lib/pgsql	100 MB	20 GB
/usr	3 GB	不适用
/opt	3 GB	不适用
/opt/puppetlabs	500 MB	不适用
/var/lib/pulp/	1 MB	300 GB
/var/lib/qpidd/	25 MB	不适用

1.3. 存储指南

安装卫星服务器以提高效率时请考虑以下指南：

- 如果您将 **/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** 已经使用 **noexec** 选项挂载，您必须将选项更改为 **exec** 并重新创建文件系统。这是 **puppetserver** 服务正常工作的要求。
- 因为大多数卫星服务器数据存储在 **/var** 目录中，因此在 LVM 存储上挂载 **/var** 可帮助系统扩展。

- **/var/lib/qpidd/** 目录使用每个由 **goferd** 服务管理的内容主机稍多 2 MB。例如，10 000 内容主机需要 **/var/lib/qpidd/** 中的磁盘空间 20 GB。
- 对 **/var/lib/pulp/** 目录使用高带宽、低延迟存储。因为红帽卫星具有大量 I/O 密集型操作，使用高延迟、低带宽存储会导致性能下降。确保您的安装有范围 60 - 80 兆字节/秒的速度。

您可以使用 **fio** 工具获取这些数据。有关使用 **fio** 工具的更多信息，请参阅 磁盘对 Satellite 操作的红帽知识库解决方案影响。

文件系统指南

- 不要使用 GFS2 文件系统作为输入输出延迟过高。

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 *Red Hat Enterprise Linux 7 系统管理员指南* 中的日志轮转。https://access.redhat.com/documentation/zh-cn/red_hat_enterprise_linux/7/html/system_administrators_guide/ch-viewing_and_managing_log_files#s2-log_rotation

日志消息所需的准确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 会阻止同步进程。要避免这种情况，请通过将以下行添加到 **/etc/fstab** 指定文件系统表中的 **/var/lib/pulp** 目录的 SELinux 上下文：

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

如果已经挂载了 NFS 共享，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

在不同存储库中重复的软件包仅在磁盘上存储一次。包含重复软件包的额外软件仓库需要较少的额外存储。批量存储驻留在 **/var/lib/pulp/** 目录中。这些端点不能手动配置。确保 **/var** 文件系统中存在存储，以防止存储问题。

Software Collections

软件集合安装在 **/opt/rh/** 和 **/opt/theforeman/** 目录中。

对于 **/opt** 目录，需要 root 用户写入和执行权限。

符号链接

您不能为 **/var/lib/pulp/** 使用符号链接。

同步的 RHEL ISO

如果您计划将 RHEL 内容 ISO 与 Satellite 同步，请注意红帽企业 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它。

1.4. 支持的操作系统

您可以从磁盘、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。只有在安装了 Satellite Server 6.10 时，仅在 Red Hat Enterprise Linux 7 服务器的最新版本上支持 Red Hat Satellite Server。以前的 Red Hat Enterprise Linux 版本（包括 EUS 或 z-stream）不被支持。

安装程序支持以下操作系统，具有软件包，并测试用于部署 Satellite 的测试：

表 1.2. satellite-installer 支持的操作系统

操作系统	架构	备注
Red Hat Enterprise Linux 7	仅限 x86_64	

在安装 Satellite 之前，请应用所有操作系统更新（如果可能）。

Red Hat Satellite Server 需要具有 **@Base** 软件包组的红帽企业 Linux 安装，无需其他软件包集修改，而且没有直接执行服务器直接操作所需的第三方配置或软件。这个限制包括强化和其他非红帽安全软件。如果您需要基础架构中的此类软件，请先安装和验证完整的卫星服务器，然后在添加任何非红帽软件前创建系统的备份。

在全新的调配的系统上安装卫星服务器。

除了运行卫星服务器之外，红帽不支持将系统用于任何其他操作。

1.5. 支持的浏览器

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

卫星 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、法语、法语和德语。

1.6. 端口和防火墙要求

若要让卫星架构的组件进行通信，请确保在基础操作系统上打开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。

使用这些信息配置任何基于网络的防火墙。请注意，某些云解决方案必须经过特别配置，以允许计算机之间的通信，因为它们隔离计算机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。如果可能，禁用应用程序检查并允许根据协议打开的端口通信。

集成胶囊

卫星服务器具有集成胶囊，并且直接连接到卫星服务器的任何主机都是本节末尾的卫星客户端。这包括运行胶囊服务器的基本操作系统。

Capsule 客户端

作为胶囊的客户端，卫星集成胶囊以外的主机不需要访问卫星服务器。如需有关卫星拓扑的更多信息，*请参阅规划红帽卫星 6 的胶囊* 联网。

所需端口可以根据您的配置进行更改。

下表指定目标端口和网络流量的方向：

表 1.3. 卫星服务器传入的流量

目标端口	协议	Service	源	必需用于	Description
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	从胶囊通信
443, 80	TCP	HTTPS、HTTP	客户端	内容接收	内容
443, 80	TCP	HTTPS、HTTP	Capsule	内容接收	内容
443, 80	TCP	HTTPS、HTTP	客户端	内容主机注册	Capsule CA RPM 安装
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
5646	TCP	AMQP	Capsule	Katello 代理	转发消息到 Qpid 分配卫星上的路由器（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	调配模板	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）

8443	TCP	HTTPS	客户端	内容主机注册	开始 上传事实 发送安装的软件包和追踪
9090	TCP	HTTPS	客户端	OpenSCAP	配置客户端
9090	TCP	HTTPS	发现的节点	Discovery（发现）	主机发现和置备
9090	TCP	HTTPS	Red Hat Satellite	Capsule API	胶囊功能

任何直接连接到卫星服务器的受管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。这包括运行胶囊服务器的基本操作系统。

DHCP 胶囊执行 ICMP ping 或 TCP 回显连接尝试尝试设置 DHCP IPAM 的子网中的主机，以找出是否考虑使用 IP 地址。可以使用 **satellite-installer --foreman-proxy-dhcp-ping-free-ip=false** 关闭此行为。

表 1.4. 卫星服务器外发流量

目标端口	协议	Service	目的地	必需用于	Description
	ICMP	ping	客户端	DHCP	免费 IP 检查（可选）
7	TCP	echo	客户端	DHCP	免费 IP 检查（可选）
22	TCP	SSH	目标主机	远程执行	运行任务
22, 16514	TCP	SSH SSH/TLS	计算资源	卫星发起的通信，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	Capsule DNS	DNS 冲突验证（可选）
53	TCP 和 UDP	DNS	DNS 服务器	编配	DNS 冲突验证
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 yum 软件仓库

389, 636	TCP	LDAP, LDAPS	外部 LDAP 服务器	LDAP	只有在启用外部身份验证时才需要 LDAP 身份验证。当定义 **LDAPAuthSource** 时，可以自定义该端口
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	cloud.redhat.com	Red Hat Cloud plugin API 调用	
443	TCP	HTTPS	Red Hat Portal	SOS 报告	协助支持问题单（可选）
443	TCP	HTTPS	Red Hat CDN	内容同步	Red Hat CDN
443	TCP	HTTPS	cert-api.access.redhat.com	Telemetry 数据上传和报告	
443	TCP	HTTPS	Capsule	内容镜像	开始
443	TCP	HTTPS	Infoblox DHCP Server	DHCP 管理	使用 Infoblox 进行 DHCP 时，管理 DHCP 租期（可选）
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）

5646	TCP	AMQP	Satellite Server	Katello 代理	将消息转发到 Qpid 分配胶囊上的路由器（可选）
5671			Qpid	远程安装	向客户端发送 install 命令
5671			分配路由器 (hub)	远程安装	转发消息在 Satellite 上分配路由器
5671			Satellite Server	适用于 Katello 代理的远程安装	向客户端发送 install 命令
5671			Satellite Server	适用于 Katello 代理的远程安装	转发消息在 Satellite 上分配路由器
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** 使用一个可配置的端口，默认为 7911 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	胶囊的管理

1.7. 启用从客户端到卫星服务器的连接

作为卫星服务器内部胶囊的客户端的胶囊和内容主机，需要通过基于卫星的主机的防火墙和任何基于网络的防火墙进行访问。

使用这个流程在安装 Satellite 的 Red Hat Enterprise Linux 7 系统上配置基于主机的防火墙，以启用来自客户端的传入连接，并使配置在系统重启后持久保留。有关使用的端口的更多信息，请参阅 端口和防火墙要求。

流程

1. 要打开客户端到 Satellite 通信的端口，请在您要在其上安装 Satellite 的基本操作系统中输入以下命令：

```
# firewall-cmd \
--add-port="80/tcp" --add-port="443/tcp" \
--add-port="5647/tcp" --add-port="8000/tcp" \
--add-port="8140/tcp" --add-port="9090/tcp" \
--add-port="53/udp" --add-port="53/tcp" \
--add-port="67/udp" --add-port="69/udp"
```

2. 使更改持久：

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

1.8. 验证防火墙设置

使用此流程验证您对防火墙设置的更改。

流程

1. 输入以下命令：

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

如需更多信息，请参阅 *Red Hat Enterprise Linux 7 安全指南* 开始使用 firewalld。

1.9. 验证 DNS 解析

使用完全限定的域名验证完整的转发和反向 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
```

成功进行名称解析会导致输出类似如下：

```
# 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. 为了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 7 网络指南中的* 使用 hostnamectl 配置主机名。

警告

名称解析对于 Satellite 6 的运作至关重要。如果卫星无法正确解析其完全限定域名，如内容管理、订阅管理和配置等任务将失败。

第 2 章 在 IPV6 网络中为 SATELLITE 安装准备您的环境

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

要在安装 Satellite 后在 IPv6 网络中置备主机，还必须为 UEFI HTTP 引导置备 Satellite。如需更多信息，请参阅在 IPv6 网络中为 UEFI HTTP 引导 Provisioning 配置 Satellite 。

2.1. IPV6 网络中 SATELLITE 安装的限制

在 IPv6 网络中安装 Satellite 有以下限制：

- 不支持在 IPv6 中安装卫星和胶囊，不支持双栈安装。
- 虽然 Satellite 调配模板包含对 PXE 和 HTTP (iPXE)调配的 IPv6 支持，但唯一测试和经认证的置备工作流是 UEFI HTTP 引导配置。这个限制仅与计划使用 Satellite 置备主机的用户相关。

2.2. IPV6 网络中进行 SATELLITE 安装的要求

在 IPv6 网络中安装 Satellite 前，请确定您满足以下要求：

- 如果您计划从卫星或胶囊置备主机，您必须在 Red Hat Enterprise Linux 版本 7.9 或更高版本上安装 Satellite 和 Capsule，因为这些版本包括 **grub2** 软件包的最新版本。
- 您必须将外部 DHCP IPv6 服务器部署为单独的非受管服务到 GRUB2 中，然后使用 DHCPv6 或分配静态 IPv6 地址来配置 IPv6 网络。这是必要的，因为 Red Hat Enterprise Linux (ISC DHCP) 中的 DHCP 服务器没有提供用于管理 IPv6 记录的集成 API，因此提供 DHCP 管理的胶囊 DHCP 插件仅限于 IPv4 子网。
- 您必须部署外部 IPv4 HTTP 代理服务器。这是必需的，因为卫星只通过 IPv4 网络分发内容，因此您必须使用 IPv4 代理将这些内容重定向到 IPv6 网络中的主机。
- 您必须将 Satellite 配置为使用此 IPv4 HTTP 代理服务器作为默认代理。如需更多信息，请参阅在 Satellite 中添加默认 HTTP 代理 。

第 3 章 安装 SATELLITE SERVER

当您从连接的网络中安装 Satellite 服务器时，您可以从 Red Hat Content Delivery Network 获取软件包并接收更新。

注意

您无法将卫星服务器注册到自己。

使用以下步骤安装卫星服务器，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 *内容管理指南中的管理订阅*。https://access.redhat.com/documentation/zh-cn/red_hat_satellite/6.10/html-single/content_management_guide/index#Managing_Subscriptions

请注意，卫星 6 安装脚本基于 Puppet，这意味着如果您多次运行安装脚本，它可能会覆盖任何手动配置更改。在执行安装脚本时，要避免这种情况并确定哪些更改应用了 **--noop** 参数。此参数可确保不进行实际的更改。潜在的更改写入到 **/var/log/foreman-installer/satellite.log**。

文件始终备份，因此您可以恢复任何不需要的更改。例如，在 foreman-installer 日志中，您可以看到类似以下有关 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. 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并消耗用户可用的订阅内容。这包括 Red Hat Enterprise Linux、Red Hat Software Collections (RHSCL)和 Red Hat Satellite 等内容。

流程

- 在 Red Hat Content Delivery Network 中注册您的系统，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
  ```

3.2. 附加 SATELLITE 基础架构订阅

注意

如果您在红帽客户门户网站中启用简单内容访问(SCA)，请跳过此部分。

注册卫星服务器后，您必须识别您的订阅池 ID 并附加可用订阅。红帽卫星基础架构订阅提供对红帽卫星、红帽企业 Linux 和红帽软件集合(RHSCL)内容的访问。这是唯一需要的订阅。

Red Hat Satellite Infrastructure 包含在所有包括 Satellite 的订阅（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，则订阅被分类为可用。如果您无法找到可用的 Satellite 订阅，请参阅红帽知识库解决方案 如何识别在 Red Hat Subscription Manager 下注册的客户端使用哪些订阅？ 运行脚本以查看您的订阅是否被其他系统消耗。

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 Ansible Engine
                     Red Hat Enterprise Linux Load Balancer (for RHEL Server)
                     Red Hat
                     Red Hat Software Collections (for RHEL Server)
                     Red Hat Enterprise Linux Server
                     Red Hat Satellite Capsule
                     Red Hat Enterprise Linux for x86_64
                     Red Hat Enterprise Linux High Availability for x86_64
                     Red Hat Satellite
                     Red Hat Satellite 5 Managed DB
                     Red Hat Satellite 6
                     Red Hat Discovery
SKU:                 MCT3719
Contract:            11878983
Pool ID:             8a85f99968b92c3701694ee998cf03b8
Provides Management: No
Available:           1
Suggested:           1
Service Level:       Premium
Service Type:        L1-L3
Subscription Type:   Standard
Ends:                03/04/2020
System 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 Infrastructure 订阅附加到 Satellite 服务器运行的基本操作系统：

```
# 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 基础架构订阅：

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

3.3. 配置软件仓库

使用此流程启用安装卫星服务器所需的存储库。从您要安装到的可用操作系统和版本列表中选择：

- Red Hat Enterprise Linux 7

3.3.1. Red Hat Enterprise Linux 7

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-7-server-rpms \
--enable=rhel-7-server-satellite-6.10-rpms \
--enable=rhel-7-server-satellite-maintenance-6-rpms \
--enable=rhel-server-rhscl-7-rpms \
--enable=rhel-7-server-ansible-2.9-rpms
```

注意

如果您要将 Satellite 服务器安装为 Red Hat Virtualization 上托管的虚拟机，还必须启用 **Red Hat Common** 软件仓库，并安装 Red Hat Virtualization 客户机代理和驱动程序。如需更多信息，请参阅 *《虚拟机管理指南》* 中的 在红帽企业 Linux 上安装客户机代理和驱动程序，了解更多信息。

3.4. 安装 SATELLITE 服务器软件包

- Red Hat Enterprise Linux 7

3.4.1. Red Hat Enterprise Linux 7

流程

1. 更新所有软件包：

```
# yum update
```

2. 安装 Satellite 服务器软件包：

```
# yum install satellite
```

3.5. 使用 CHRONYD 同步系统时钟

要最小化时间偏差的效果，您必须在要安装带有网络时间协议(NTP)服务器的基本操作系统上同步系统时钟。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 7 系统管理员* 指南中的使用 chrony Suite 配置 NTP。

流程

1. 安装 **chrony** 软件包：

```
# yum install chrony
```

2. 启动并启用 **chronyd** 服务：

```
# systemctl start chronyd
# systemctl enable chronyd
```

3.6. 在基本操作系统上安装 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 系统收集配置和诊断信息。您还可以使用它提供初始系统分析，使用红帽技术支持打开服务请求时是必需的。有关使用 **sos** 的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 4.6 及之后的版本中创建？

流程

1. 安装 **sos** 软件包：

```
# yum install sos
```

3.7. 配置 SATELLITE 服务器

使用 **satellite-installer** 安装脚本安装卫星服务器。

此方法通过运行一个或多个命令选项来执行。命令选项覆盖对应的默认初始配置选项，并在卫星应答文件中记录。您可以根据需要尽可能地运行 脚本来配置任何必要的选项。

注意

根据您运行 Satellite 安装程序时使用的选项，配置可能需要几分钟来完成。

3.7.1. 配置 Satellite

这个初始配置过程会创建一个机构、位置、用户名和密码。在初始配置后，如果需要，您可以创建其他组织和位置。初始配置还会在同一服务器上安装 PostgreSQL 数据库。

完成安装过程可能需要十分钟时间。如果您要远程登录系统，请使用 **屏幕** 或 **tmux** 等工具允许暂停和重新连接通信会话，以便在与远程系统断开连接时检查安装进度。Red Hat 知识库文章 如何使用 **screen** 命

令 描述安装屏幕 ; 另外，**屏幕** man page 了解更多信息。如果您丢失了安装命令运行的 shell 的连接，请参阅 **/var/log/foreman-installer/satellite.log** 中的日志，以确定进程是否成功完成。

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，则创建一个名为 **Default Organization** 的组织，标签为 **Default_Organization**。您可以重命名机构名称，但不能重命名标签。
- 远程执行是管理内容主机上软件包的主要方法。如果要使用已弃用的 Katello Agent 而不是 Remote Execution SSH，请使用 **--foreman-proxy-content-enable-katello-agent=true** 选项来启用它。应在任何胶囊服务器以及卫星服务器上提供相同的选项。
- 默认情况下，安装程序配置的所有配置文件都由 Puppet 管理。当 **satellite-installer** 运行时，它会使用初始值覆盖对 Puppet 管理的文件的任何手动更改。默认情况下，卫星服务器将与作为服务运行的 Puppet 代理一起安装。如果需要，您可以使用 **--puppet-runmode=none** 选项来禁用卫星服务器上的 Puppet 代理。
- 如果要手动管理 DNS 文件和 DHCP 文件，请使用 **--foreman-proxy-dns-managed=false** 和 **--foreman-proxy-dhcp-managed=false** 选项，以便 Puppet 不会管理与对应服务相关的文件。有关如何在其他服务 上应用自定义配置的更多信息，请参阅将自定义配置应用到卫星。

流程

1. 使用以下命令，包括您要使用的任何附加选项：

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

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

3.8. 将订阅清单导入到卫星服务器

使用以下步骤将订阅清单导入到卫星服务器。

前提条件

- 您必须具有从客户门户网站中导出的订阅清单文件。如需更多信息， *请参阅使用 Red Hat Subscription Management 指南中的使用清单*。

流程

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

4. 导航到包含 Subscription Manifest 文件的位置，然后单击 **Open**。如果 Manage Manifest 窗口没有自动关闭，点 **Close** 来返回订阅窗口。

CLI 过程

1. 将订阅清单文件从客户端复制到 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，再导入订阅清单文件：

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

第 4 章 在卫星服务器上执行额外的配置

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，以及性能降级和稳定性问题。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，查看影响和解析的详细信息，然后确定受影响的系统。

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

为了维护您的卫星服务器，并改进您使用卫星监控和诊断问题的能力，在卫星服务器上安装红帽卫星，并将卫星服务器注册到 Red Hat Insights。

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 服务器中安装 Red Hat Insights，请输入以下命令：

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

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

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

4.2. 禁用 RED HAT INSIGHTS 的注册

安装或升级 Satellite 后，您可以选择根据需要取消注册或注册 Red Hat Insights。例如，如果需要在断开连接的环境中使用 Satellite，您可以从卫星服务器取消注册 **insights-client**。

前提条件

1. 您已在红帽客户门户中注册了 Satellite。

流程

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

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

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

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

4.3. 启用 SATELLITE TOOLS 6.10 存储库

Satellite Tools 6.10 存储库提供 **katello-agent**、**katello-host-tools**，以及用于注册到卫星服务器的客户端的 **puppet** 软件包。

要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

流程

1. 在 Satellite Web UI 中，导航到 **Content** > **Red Hat Repositories**。
2. 使用 Search 字段输入以下存储库名称： **Satellite Tools 6.10 （适用于 RHEL 7 服务器） (RPMs)**。
3. 在 Available Repositories 窗格中，点 **Satellite Tools 6.10 （用于 RHEL 7 Server）(RPMs)**以展开存储库集。
   如果 **Satellite Tools 6.10** 项目不可见，则可能是因为从客户门户网站获取的订阅清单中不包含它们。要更正，登录到客户门户网站，添加这些软件仓库，下载订阅清单并导入到卫星中。
4. 对于 **x86_64** 条目，请单击 **Enable** 图标以启用该存储库。

为主机上运行的每个支持的 Red Hat Enterprise Linux 主版本启用 Satellite Tools 6.10 软件仓库。启用红帽存储库后，将自动创建此存储库的产品。

CLI 过程

- 使用 **hammer repository-set enable** 命令启用 Satellite Tools 6.10 存储库：

```
# hammer repository-set enable --organization "initial_organization_name" \
--product 'Red Hat Enterprise Linux Server' \
--basearch='x86_64' \
--name 'Red Hat Satellite Tools 6.10 (for RHEL 7 Server) (RPMs)'
```

4.4. 同步 SATELLITE TOOLS 6.10 存储库

使用这个部分将 Satellite Tools 6.10 存储库从 Red Hat Content Delivery Network (CDN)同步到 Satellite。此存储库为注册到卫星服务器的客户端提供 **katello-agent**、**katello-host-tools** 和 **puppet** 软件包。

流程

1. 在 Satellite Web UI 中，进入 **Content** > **Sync Status**。
   此时会显示可用于同步的产品存储库列表。
2. 点击 **Red Hat Enterprise Linux Server**产品旁边的箭头来查看可用的内容。
3. 选择 **Satellite Tools 6.10 （适用于 RHEL 7 服务器）RPM x86_64**。
4. 单击 **Synchronize Now**。

CLI 过程

- 使用 **hammer 存储库同步您的 Satellite Tools 6.10 存储库** ：

```
# hammer repository synchronize --organization "initial_organization_name" \
--product 'Red Hat Enterprise Linux Server' \
--name 'Red Hat Satellite Tools 6.10 for RHEL 7 Server RPMs x86_64' \
--async
```

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 网络中的主机。

前提条件

- 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 服务。
- 确保为客户端打开 TCP 端口 8000，以便客户端从卫星和胶囊下载文件和 Kickstart 模板。
- 确保主机置备接口子网具有 HTTP 引导胶囊，并且已设置 Templates Capsule。有关更多信息，请参阅 *《调配指南》* 中的 将子网添加到卫星服务器。
- 导航到 **Administer** > **Settings** > **Provisioning**，并确保 **Token duration** 设置没有设置为 0。**卫星无法识别通过远程 IPv6 地址从网络引导的客户端，因为托管 DHCPv6 服务，因此必须启用置备令牌。**

流程

1. **您必须在安装程序中禁用 DHCP 管理，或使用它。**
2. **对于在卫星中创建的所有 IPv6 子网，请将 DHCP 胶囊 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 中，将 grub2-efi 软件包更新至最新版本：**

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

5. **同步 Red Hat Enterprise Linux 8 kickstart 软件仓库。**

4.6. 使用 HTTP 代理配置 SATELLITE 服务器

使用以下步骤为 Satellite 配置 HTTP 代理。

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 服务器配置为使用 HTTP 代理来请求发送到 Red Hat Content Delivery Network (CDN)或其他内容源。在可能的情况下，使用 FQDN 而不是 IP 地址，以避免因为网络更改而丢失连接。

以下流程只为 Satellite 下载内容配置代理。要使用 CLI 而不是 Web UI，请参阅 CLI 过程。

流程

1. **在 Satellite Web UI 中，导航到 Infrastructure >HTTP Proxies。**
2. **点 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，在 Username 字段中输入要进行身份验证的用户名。
6. 可选： 如果需要验证，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，请单击 Test Connection 按钮。
8. 点 Submit。
9. 导航到 Administer >Settings，然后点 Content 选项卡。
10. 将默认 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** 变量是否已设置。

```
# 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. 将 HTTP 代理配置为连接到红帽 CDN

验证 Satellite 是否可以连接到红帽 CDN，并可同步其存储库。

流程

1. 在网络网关和 HTTP 代理上，为以下主机名启用 TCP：

主机名	端口	协议
subscription.rhsm.redhat.com	443	HTTPS
cdn.redhat.com	443	HTTPS
*.akamaiedge.net	443	HTTPS
cert.cloud.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

主机名	端口	协议
api.access.redhat.com （如果使用 Red Hat Insights）	443	HTTPS

卫星服务器使用 SSL 安全地与红帽 CDN 通信。使用 SSL 拦截器代理会干扰这个通信。这些主机必须在代理上列在白名单中。

有关 Red Hat CDN (cdn.redhat.com)使用的 IP 地址列表，请查看红帽客户门户网站中的知识库文章公共 CIDR 列表。

2. 在卫星服务器上，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 =
```

4.6.3. 配置 SELinux 以确保访问自定义端口

SELinux 可确保仅在特定端口访问 Red Hat Satellite 6 和 Red Hat Subscription Manager。对于 HTTP 缓存，TCP 端口为 8080、8118、8123 和 10001 - 10010。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 允许用于 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，请输入以下命令：

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

4.6.4. 在所有 Satellite HTTP 请求中使用 HTTP 代理

如果您的卫星服务器必须保持在阻止 HTTP 和 HTTPS 的防火墙后面，您可以配置代理以用于与外部系统通信，包括计算资源。

请注意，如果您使用计算资源进行置备，并且您希望使用与计算资源使用不同的 HTTP 代理，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，导航到 Administer > Settings。
2. 在 HTTP (S)代理 行中，选择相邻值 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
```

4.6.5. 从接收已发出的请求中排除主机

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，导航到 Administer > Settings。
2. 在 HTTP (S)代理（除 hosts 行外），选择相邻值 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...]
```

4.6.6. 重置 HTTP 代理

如果要重置当前 HTTP 代理服务器设置，请取消设置默认 HTTP Proxy 设置。

流程

1. 导航到 Administer > Settings，然后点 Content 选项卡。
2. 将默认 HTTP 代理服务器 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. 在受管主机上启用电源管理

要使用智能平台管理接口(IPMI)或类似的协议对受管主机执行电源管理任务，您必须在卫星服务器上启用基板管理控制器(BMC)模块。

前提条件

- **所有受管主机都必须具有 BMC 类型的网络接口。卫星服务器使用此 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. 在卫星服务器上配置 DNS、DHCP 和 TFTP

要在卫星服务器上配置 DNS、DHCP 和 TFTP 服务，请使用 satellite-installer 命令以及适合您的环境的选项。要查看可配置的选项列表，请输入 satellite-installer --scenario satellite --help 命令。

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，每次使用更改的值更新所有配置文件。

要使用外部 DNS、DHCP 和 TFTP 服务，请参阅 第 5 章 *使用外部服务配置 Satellite 服务器*。

添加多主页 DHCP 详情

如果要使用多主页 DHCP，您必须通知安装程序。

前提条件

- **确定可用的以下信息如下：**
  - **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，使用 FQDN 而不是 IP 地址。**
- **请联系您的网络管理员以确保您具有正确的设置。**

流程

- **输入 satellite-installer 命令，并适合您的环境。以下示例显示了配置完整置备服务：**

```
# satellite-installer --scenario satellite \
--foreman-proxy-dns true \
--foreman-proxy-dns-managed true \
--foreman-proxy-dns-interface eth0 \
--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-interface eth0 \
--foreman-proxy-dhcp-additional-interfaces eth1 \
--foreman-proxy-dhcp-additional-interfaces eth2 \
--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
```

您可以监控在您的提示符中显示的 satellite-installer 命令的进度。您可以在 /var/log/foreman-installer/satellite.log 中查看日志。您可以在 /etc/foreman-installer/scenarios.d/satellite-answers.yaml 文件中查看使用的设置，包括 initial_admin_password 参数。

有关配置 DHCP、DNS 和 TFTP 服务的更多信息，请参阅 *《调配指南》* 中的配置网络服务 部分。

4.9. 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，您必须阻止 Satellite 在操作系统中维护这些服务，并禁用编排以避免 DHCP 和 DNS 验证错误。但是，卫星不会删除操作系统上的后端服务。

流程

1. **在卫星服务器上，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，导航到 Infrastructure >Subnets 并选择 subnet。**
3. **单击 Capsules 选项卡，清除 DHCP Capsule、TFTP Capsule 和 Reverse DNS Capsule 字段。**
4. **导航到 Infrastructure >Domains 并选择一个域。**
5. **清除 DNS Capsule 字段。**
6. **可选：如果您使用第三方提供的 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，卫星 6 不会执行编排。在启用或禁用胶囊关联时，如果不存在预期的记录和配置文件，现有主机的编配命令可能会失败。当关联胶囊以打开编配时，请确保所需的 DHCP 和 DNS 记录以及 TFTP 文件已用于现有的 Satellite 主机，以防止未来出现主机删除失败。

4.10. 配置卫星服务器以进行 OUTGOING 电子邮件

要从卫星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

- **某些包含反垃圾邮件保护或问候功能的 SMTP 服务器已知可导致问题。使用此类服务设置传出电子邮件，可以在卫星服务器上安装和配置 vanilla SMTP 服务以进行转发，或者使用 sendmail 命令。**

流程

1. **在卫星 Web UI 中，导航到 Administer → Settings。**
2. 单击 **Email** 选项卡，再设置配置选项以匹配您首选的发送方法。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 服务器作为交付方法

名称	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

名称	示例值
交付方法	SMTP
SMTP 地址	smtp.gmail.com
SMTP 身份验证	plain
SMTP HELO/EHLO 域	smtp.gmail.com
SMTP 启用 StartTLS auto	是

名称	示例值
SMTP 密码	*password*
SMTP 端口	587
SMTP 用户名	*user*@gmail.com

c. **以下示例使用 sendmail 命令作为交付方法：**

表 4.3. 使用 sendmail 作为交付方法

名称	示例值
交付方法	sendmail
Sendmail 参数	-i -t -G

Sendmail 参数指定传递给 sendmail 命令的选项。默认值为 -i -t。详情请查看 sendmail 1 man page。

3. **如果您决定使用 TLS 身份验证的 SMTP 服务器发送电子邮件，并执行以下步骤之一：**

- **将 SMTP 服务器的 CA 证书标记为 trusted。要做到这一点，请在 Satellite 服务器中执行以下命令：**

```
# 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 web UI 中，将 SMTP 启用 StartTLS auto 选项设为 No。**

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

注意

有关为个人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* 中配置电子邮件通知。

4.11. 为 SATELLITE 配置 ALTERNATE CNAME

您可以为 Satellite 配置备用 CNAME。如果您要将卫星 Web 界面部署到与客户端系统用于连接卫星时使用的域名不同的域名上，这可能会很有用。在安装胶囊和将主机注册到卫星之前，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。

4.11.1. 使用 Alternate CNAME 配置 Satellite

使用此流程为 Satellite 配置备用 CNAME。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 Satellite 并想使用备用 CNAME 配置卫星，请在卫星上输入以下命令来生成具有额外 CNAME 的新默认卫星 SSL 证书。

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

- 如果您尚未安装 Satellite，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，将备用 CNAME 记录包含在自定义证书中。如需更多信息，请参阅为卫星服务器 创建自定义 SSL 证书。

4.11.2. 将主机配置为使用 Alternate Satellite CNAME 进行内容管理

如果卫星配置了备用 CNAME，您可以将主机配置为使用备用卫星 CNAME 进行内容管理。为此，您必须在将主机注册到卫星服务器前将主机指向备用卫星 CNAME。您可以使用 bootstrap 脚本或手动完成此操作。

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 主机名和 **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。

4.12. 使用自定义 SSL 证书配置 SATELLITE 服务器

默认情况下，红帽卫星 6 使用自签名 SSL 证书来启用卫星服务器、外部胶囊服务器和所有主机之间的加密通信。如果无法使用卫星自签名证书，您可以将卫星服务器配置为使用由外部证书颁发机构签名的 SSL 证书。

要使用自定义证书配置 Satellite 服务器，请完成以下步骤：

1. 第 4.12.1 节 “为卫星服务器创建自定义 SSL 证书”
2. 第 4.12.2 节 “将自定义 SSL 证书部署到卫星服务器”
3. 第 4.12.3 节 “将自定义 SSL 证书部署到主机”
4. 如果将外部胶囊服务器注册到卫星服务器，则必须使用自定义 SSL 证书来配置它们。相同的证书颁发机构必须签署卫星服务器和胶囊服务器的证书。有关更多信息，请参阅在安装胶囊服务器中使用自定义 SSL *证书*配置胶囊服务器。

4.12.1. 为卫星服务器创建自定义 SSL 证书

使用此流程为卫星服务器创建自定义 SSL 证书。如果您已经有适用于卫星服务器的自定义 SSL 证书，请跳过此步骤。

使用自定义证书配置 Satellite 服务器时，请注意以下注意事项：

- 您必须将 Privacy-Enhanced Mail (PEM)编码用于 SSL 证书。
- 您不能对卫星服务器和胶囊服务器使用相同的证书。
- 相同的证书颁发机构必须签署卫星服务器和胶囊服务器的证书。

流程

1. 要存储所有源证书文件，请创建一个只可由 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。如果您使用受密码保护的私钥，请删除私钥密码。

   如果您已拥有此卫星服务器的私钥，请跳过这一步。

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

3. 为证书签名请求(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
x509_extensions = usr_cert
prompt = no

[ req_distinguished_name ] 1
C  = Country Name (2 letter code)
ST = State or Province Name (full name)
L  = Locality Name (eg, city)
O  = Organization Name (eg, company)
OU = The division of your organization handling the certificate
CN = satellite.example.com 2

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
```

```
extendedKeyUsage = serverAuth, clientAuth, codeSigning, emailProtection
subjectAltName = @alt_names

[ usr_cert ]
basicConstraints=CA:FALSE
nsCertType = client, server, email
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth, codeSigning, emailProtection
nsComment = "OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

[ alt_names ]
DNS.1 = satellite.example.com (3)
```

1. **在 [req_distinguished_name] 部分中，输入有关您的机构的信息。**
2. **将证书的通用名称 CN 设置为与卫星服务器的完全限定域名(FQDN)匹配。若要确认 FQDN，可在该卫星服务器上输入 hostname -f 命令。这需要确保 katello-certs-check 命令正确验证证书。**
3. **将 Subject Alternative Name (SAN) DNS.1 设置为与您的服务器的完全限定域名(FQDN)匹配。**

4. **生成证书签名请求(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. **到配置文件的路径。**
3. **要生成的 CSR 的路径。**

5. **将证书签名请求发送到证书颁发机构。相同的证书颁发机构必须签署卫星服务器和胶囊服务器的证书。**
   提交请求时，指定证书的 lifespan。发送证书请求的方法会有所不同，因此请查阅证书颁发机构来获得首选方法。为响应请求，预计可在单独的文件中接收证书颁发机构捆绑包和签名证书。

4.12.2. 将自定义 SSL 证书部署到卫星服务器

使用此流程将卫星服务器配置为使用由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，并将自定义 SSL 证书部署到卫星服务器所需的命令返回。

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)必须与卫星服务器的 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卫星服务器证书文件的路径。
2. 用于签署卫星服务器证书的私钥的路径。
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，其中一个命令必须使用它来将证书部署到卫星服务器。

要使用自定义证书安装 Red Hat Satellite 服务器，请运行：

```
satellite-installer --scenario satellite \
  --certs-server-cert "/root/satellite_cert/satellite.example.com_cert.pem" \
  --certs-server-key "/root/satellite_cert/satellite.example.com_cert_key.pem" \
  --certs-server-ca-cert "/root/satellite_cert/CA-Chain.pem"
```

要更新当前运行的 Satellite 安装中的证书，请运行：

```
satellite-installer --scenario satellite \
  --certs-server-cert "/root/satellite_cert/satellite.example.com_cert.pem" \
  --certs-server-key "/root/satellite_cert/satellite.example.com_cert_key.pem" \
  --certs-server-ca-cert "/root/satellite_cert/CA-Chain.pem" \
  --certs-update-server \
  --certs-update-server-ca
```

2. 根据您的要求，输入 satellite-installer 命令，该命令使用自定义 SSL 证书安装新的卫星服务器，或在当前运行的卫星服务器上更新证书。在某些情况下，katello-certs-check 命令的输出可能并不准确。因此，您必须遵循上述步骤，而不是命令输出。
   如果您不确定要运行哪些命令，可以通过检查 /etc/foreman-installer/scenarios.d/.installed.d/.installed 文件来验证是否安装了卫星。如果文件存在，请运行更新证书的第二个 satellite-installer 命令。

重要

部署证书后，请勿删除证书存档文件。例如，在升级卫星服务器时，需要它。

3. 在有网络访问卫星服务器的计算机中，导航到以下 URL：\https://*satellite.example.com*。
4. 在浏览器中，查看证书详情以验证部署的证书。

4.12.3. 将自定义 SSL 证书部署到主机

将卫星服务器配置为使用自定义 SSL 证书后，您还必须在注册到此卫星服务器的每个主机上安装 katello-ca-consumer 软件包。

流程

- 在每个主机上，安装 katello-ca-consumer 软件包：

```
# yum localinstall \
http://satellite.example.com/pub/katello-ca-consumer-latest.noarch.rpm
```

4.13. 将外部数据库与 SATELLITE 搭配使用

作为红帽卫星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。在某些卫星部署中，使用外部数据库而不是默认的本地数据库可帮助服务器负载。

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

要在 Satellite 中创建和使用外部数据库，您必须完成以下步骤：

1. 第 4.13.2 节 “为外部数据库准备主机”.准备红帽企业 Linux 7 服务器以托管外部数据库。
2. 第 4.13.3 节 “安装 PostgreSQL”.使用卫星、Candlepin 和 Pulp 为 PostgreSQL 准备 PostgreSQL，以及拥有它们的专用用户。
3. 第 4.13.4 节 “将 Satellite 配置为使用外部数据库”.编辑 **satellite-installer** 参数以指向新数据库，并运行 **satellite-installer**。

4.13.1. 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卫星配置：Satellite 支持 PostgreSQL 版本 12.1。

外部 PostgreSQL 的优点：

- 增加 Satellite 上的可用内存和可用 CPU
- 将 PostgreSQL 数据库上的 **shared_buffers** 设置为高灵活性，不会造成与 Satellite 上的其他服务干扰的风险
- 在不影响 Satellite 操作的情况下，调整 PostgreSQL 服务器系统的灵活性

外部 PostgreSQL 的缺点

- 增加部署复杂性，这会增加故障排除的难度
- 外部 PostgreSQL 服务器是另一个要修补和维护的系统
- 如果 Satellite 或 PostgreSQL 数据库服务器出现硬件或存储故障，则 Satellite 无法正常工作
- 如果卫星服务器和数据库服务器之间存在延迟，性能可能会受到影响

如果您怀疑 Satellite 中的 PostgreSQL 数据库造成性能问题，请使用 Satellite 6 中的信息：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大型安装的性能问题导致的，并移到外部数据库可能并不能提供帮助。如果您的查询缓慢，请联系红帽支持。

4.13.2. 为外部数据库准备主机

使用最新的 Red Hat Enterprise Linux 7 服务器安装一个新的置备系统，以托管外部数据库。

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

前提条件

- 红帽企业 Linux 7 服务器必须满足卫星 的存储要求。

流程

1. 使用 Attaching Satellite Infrastructure Subscription 中的说明将 Satellite 订阅附加到您的服务器。
2. 禁用所有软件仓库并只启用以下软件仓库：

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

4.13.3. 安装 PostgreSQL

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

流程

1. 要安装 PostgreSQL，请输入以下命令：

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

2. 要初始化 PostgreSQL，请输入以下命令：

```
# postgresql-setup initdb
```

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

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

4. 删除 **#** 和 edit 以侦听入站连接：

```
listen_addresses = '*'
```

5. Edit the **/var/opt/rh/rh-postgresql12/lib/pgsql/data/pg_hba.conf** file:

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

6. 在文件中添加以下行：

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

7. 要启动并启用 PostgreSQL 服务，请输入以下命令：

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

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

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

9. 切换到 postgres 用户并启动 PostgreSQL 客户端：

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

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

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

11. 退出 postgres 用户：

```
# \q
```

12. 从卫星服务器，测试您可以访问数据库。如果连接成功，命令会返回 1。

```
# PGPASSWORD='Foreman_Password' psql -h postgres.example.com  -p 5432 -U foreman
-d foreman -c "SELECT 1 as ping"
# PGPASSWORD='Candlepin_Password' psql -h postgres.example.com -p 5432 -U
candlepin -d candlepin -c "SELECT 1 as ping"
# PGPASSWORD='Pulpcore_Password' psql -h postgres.example.com -p 5432 -U pulp -d
pulpcore -c "SELECT 1 as ping"
```

4.13.4. 将 Satellite 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 服务器中安装和配置了 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-host postgres.example.com \
  --foreman-db-password Foreman_Password \
  --foreman-db-database foreman \
  --foreman-db-manage false \
```

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

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

4.14. 使用预定义的配置集调整卫星服务器

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改进 Satellite 的性能。

请注意，您不能在胶囊上使用调优配置文件。

您可以根据 Satellite 管理和支持硬件资源的主机数量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，部署配置设置会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. **您要应用于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，则 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，以及 /etc/foreman-installer/custom-hiera.yaml 文件，并从 /etc/foreman-installer/custom-hiera.yaml 文件中删除任何重复的配置。

default

受管主机数量： 0-5000
RAM：20G

CPU 内核数： 4

中

受管主机数量：5001-10000
RAM：32G

CPU 内核数：8

大

受管主机数量： 10001-20000
RAM：64G

CPU 内核数：16

extra-large

受管主机数量： 20001-60000
RAM: 128G

CPU 内核数：32

extra-extra-large

受管主机数量：60000+
RAM：256G

CPU 内核数： 48+

流程

1. **可选：如果您已在 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。如果备份文件被破坏，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：如果您已在 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 以及要在 /usr/share/foreman-installer/config/foreman.hiera/tuning/tuning/tuning/sizes/tuning/tuning/size 中应用的默认调优配置文件的定义。将配置条目与 /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. **输入您要应用的 profile 的 --tuning 选项的 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 5 章 使用外部服务配置 SATELLITE 服务器

如果不想在卫星服务器上配置 DNS、DHCP 和 TFTP 服务，请使用本节将卫星服务器配置为使用外部 DNS、DHCP 和 TFTP 服务。

5.1. 使用外部 DNS 配置 SATELLITE 服务器

您可以使用外部 DNS 配置卫星服务器。卫星服务器使用 nsupdate 工具更新远程服务器上的 DNS 记录。

要永久保留任何更改，您必须输入 satellite-installer 命令以及适合您的环境的选项。

前提条件

- **您必须有配置了外部 DNS 服务器。**

流程

1. **解锁软件包以启用新软件包的安装：**

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

2. **安装 BIND 和实用程序软件包：**

```
# yum install bind bind-utils
```

3. **锁定软件包：**

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

4. **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/rndc.key
```

5. **配置所有权、权限和 SELinux 上下文：**

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

6. **要测试 nsupdate 工具，请远程添加主机：**

```
# echo -e "server DNS_IP_Address\n \
update add aaa.virtual.lan 3600 IN A Host_IP_Address\n \
send\n" | nsupdate -k /etc/rndc.key
# nslookup aaa.virtual.lan DNS_IP_Address
# echo -e "server DNS_IP_Address\n \
update delete aaa.virtual.lan 3600 IN A Host_IP_Address\n \
send\n" | nsupdate -k /etc/rndc.key
```

7. **手动将 foreman-proxy 用户分配给指定组。通常，satellite-installer 可确保 foreman-proxy 用户属于指定的 UNIX 组，但是在这种情况下，卫星不管理用户和组，因此您需要将 foreman-proxy 用户手动分配给指定组。**

```
# usermod -a -G named foreman-proxy
```

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

```
# 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/rndc.key \
--foreman-proxy-dns-ttl=86400
```

9. 重启 **foreman-proxy** 服务：

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

10. 登录卫星服务器 **Web UI**。

11. 导航到 **Infrastructure > Capsules**，找到 **Satellite Server**，然后从 **Actions** 列中的列表中，选择 **Refresh**。

12. 将 **DNS** 服务与适当的子网和域关联。

5.2. 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 5.2.1 节 “将外部 DHCP 服务器配置为与卫星服务器一起使用”

2. 第 5.2.2 节 “使用外部 DHCP 服务器配置 Satellite 服务器”

5.2.1. 将外部 DHCP 服务器配置为与卫星服务器一起使用

要配置外部 DHCP 服务器以用于 Satellite 服务器，必须在 Red Hat Enterprise Linux 服务器中安装 ISC DHCP Service 和 Berkeley Internet Name Domain (BIND)软件包。您还需要与卫星服务器共享

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，因为卫星会在 TFTP 服务器上创建 grub2/ 子目录的配置文件。如果禁用了 dhcp-no-override 设置，客户端会从根目录获取启动加载器及其配置，这可能会导致错误。

流程

1. 在 Red Hat Enterprise Linux 服务器服务器中，安装 ISC DHCP Service 和 Berkeley Internet Name Domain (BIND)软件包：

```
# yum install dhcp bind
```

2. 生成安全令牌：

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

因此，在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：

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

4. 编辑所有子网的 dhcpd 配置文件并添加该密钥。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 "jNSE5YI3H1A8Oj/tkV4...A2ZOHb6zv315CkNAY7DMYYCj48Umw==";
};
omapi-key omapi_key;
```

请注意，选项路由器 值是您要用于外部 DHCP 服务的卫星或胶囊 IP 地址。

5. 从在其中创建的目录中删除这两个密钥文件。

6. 在卫星服务器上，定义各个子网。暂时不要为定义的子网设置 DHCP 胶囊。

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，在卫星 Web UI 中将保留范围定义为 192.168.38.101 到 192.168.38.250。

7. 配置外部对 DHCP 服务器的防火墙：

```
# firewall-cmd --add-service dhcp \
&& firewall-cmd --runtime-to-permanent
```

8. 在卫星服务器上，确定 foreman 用户的 UID 和 GID：

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

9. 在 DHCP 服务器上，使用与上一步中确定相同的 ID 创建 foreman 用户和组：

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

10. 为确保配置文件可以访问，请恢复读取和执行标志：

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

11. 启动 **DHCP** 服务：

```
# systemctl start dhcpd
```

12. 使用 **NFS** 导出 **DHCP** 配置和租期文件：

```
# yum install nfs-utils
# systemctl enable rpcbind nfs-server
# systemctl start rpcbind nfs-server nfs-lock nfs-idmapd
```

13. 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
```

14. 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
```

15. 在 **/etc/fstab** 中挂载文件系统：

```
# mount -a
```

16. 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** 地址是卫星或胶囊 **IP** 地址，您要用于外部 **DHCP** 服务。

17. 重新载入 **NFS** 服务器：

```
# exportfs -rva
```

18. 配置 DHCP omapi 端口 7911 的防火墙：

```
# firewall-cmd --add-port="7911/tcp" \
&& firewall-cmd --runtime-to-permanent
```

19. 可选：配置对 NFS 外部访问的防火墙。客户端使用 NFSv3 配置。

```
# firewall-cmd --zone public --add-service mountd \
&& firewall-cmd --zone public --add-service rpc-bind \
&& firewall-cmd --zone public --add-service nfs \
&& firewall-cmd --runtime-to-permanent
```

5.2.2. 使用外部 DHCP 服务器配置 Satellite 服务器

您可以使用外部 DHCP 服务器配置卫星服务器。

前提条件

- 确保您已配置了一个外部 DHCP 服务器，并且已与卫星服务器共享 DHCP 配置和租期文件。更多信息请参阅 第 5.2.1 节 “将外部 DHCP 服务器配置为与卫星服务器一起使用”。

流程

1. 安装 nfs-utils 工具：

```
# yum 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 文件中添加以下几行：**

```
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 上挂载文件系统：**

```
# mount -a
```

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

```
# su foreman-proxy -s /bin/bash
bash-4.2$ cat /mnt/nfs/etc/dhcp/dhcpd.conf
bash-4.2$ cat /mnt/nfs/var/lib/dhcpd/dhcpd.leases
bash-4.2$ exit
```

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

```
# satellite-installer --foreman-proxy-dhcp=true \
--foreman-proxy-dhcp-provider=remote_isc \
--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=jNSE5YI3H1A8Oj/tkV4...A2ZOHb6zv315CkNAY7DMYYCj48Umw== \
--foreman-proxy-plugin-dhcp-remote-isc-omapi-port=7911 \
--enable-foreman-proxy-plugin-dhcp-remote-isc \
--foreman-proxy-dhcp-server=DHCP_Server_FQDN
```

9. **重启 foreman-proxy 服务：**

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

10. **登录卫星服务器 Web UI。**

11. 导航到 **Infrastructure > Capsules**，找到 **Satellite Server**，然后从 **Actions** 列中的列表中，选择 **Refresh**。

12. 将 **DHCP** 服务与适当的子网和域关联。

5.3. 使用外部 TFTP 配置 SATELLITE 服务器

您可以使用外部 **TFTP** 服务配置卫星服务器。

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** 文件进行以下持久更改：

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

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. 登录卫星服务器 Web UI。

7. 导航到 Infrastructure > Capsules，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。

5.4. 使用外部 IDM DNS 配置 SATELLITE 服务器

当卫星服务器为主机添加 DNS 记录时，它会首先确定哪个胶囊为该域提供 DNS。然后，它将与配置为为您的部署提供 DNS 服务的胶囊通信并添加记录。此过程中不涉及主机。因此，您必须在卫星或胶囊上安装并配置 IdM 客户端，以便为您要使用 IdM 服务器管理的域提供 DNS 服务。

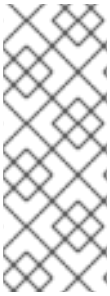
卫星服务器可以配置为使用 Red Hat Identity Management (IdM)服务器来提供 DNS 服务。有关红帽身份管理的更多信息，请参阅 Linux 域身份、身份验证和策略指南。

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，请使用以下步骤之一：

- 第 5.4.1 节 “使用 GSS-TSIG 身份验证配置动态 DNS 更新”
- 第 5.4.2 节 “使用 TSIG 身份验证配置动态 DNS 更新”

要恢复到内部 DNS 服务，请使用以下步骤：

- 第 5.4.3 节 “恢复到内部 DNS 服务”



注意

您不需要使用卫星服务器来管理 DNS。当您使用 Satellite 的域注册功能（其中置备的主机自动注册到 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 服务器是相互排斥的。有关配置域注册的更多信息，请参阅 *管理 Red Hat Satellite 中的 Provisioned Hosts 的外部身份验证*。

5.4.1. 使用 GSS-TSIG 身份验证配置动态 DNS 更新

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

前提条件

- 您必须确保部署 IdM 服务器，且正确配置了基于主机的防火墙。有关更多信息，请参阅 *Linux 域身份、身份验证和策略指南中的*端口要求。
- 您必须联系 IdM 服务器管理员，以确保获取 IdM 服务器上的帐户，并具有在 IdM 服务器中创建区的权限。
- 您必须确认卫星服务器或胶囊服务器是否已配置为为您的部署提供 DNS 服务。
- 您必须在管理部署的 DNS 服务 Satellite 或 Capsule 基础操作系统上配置 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 配置卫星服务器。

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了一个 Kerberos ticket：

```
# kinit idm_user
```

2. 为卫星服务器创建一个新的 Kerberos 主体，以用于在 IdM 服务器中进行身份验证。

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

安装和配置 IdM 客户端

1. 在管理部署的 DNS 服务的 Satellite 或 Capsule 的基本操作系统上，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来配置 IdM 客户端：

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

3. 获取Kerberos ticket：

```
# kinit admin
```

4. 删除任何预先存在的 keytab ：

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

5. 获取此系统的 keytab:

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

注意

当在服务中使用与原始系统相同的主机名添加 keytab 系统时，添加 r 选项以防止生成新凭证并在原始系统中呈现凭证无效。

6. 对于 dns.keytab 文件，请将组和拥有者设置为 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开的列表：**

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

   e. **将 Dynamic update 设置为 True。**

   f. **启用 允许 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 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开的列表：**

```
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 服务的卫星或胶囊服务器

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=true \
--foreman-proxy-dns-managed=true \
--foreman-proxy-dns-provider=nsupdate_gss \
--foreman-proxy-dns-server="idm1.example.com" \
--foreman-proxy-dns-tsig-principal="capsule/satellite.example.com@EXAMPLE.COM" \
--foreman-proxy-dns-tsig-keytab=/etc/foreman-proxy/dns.keytab \
--foreman-proxy-dns-reverse="55.168.192.in-addr.arpa" \
--foreman-proxy-dns-zone=example.com \
--foreman-proxy-dns-ttl=86400
```

- **在 Capsule 上输入以下命令：**

```
satellite-installer --scenario capsule \
--foreman-proxy-dns=true \
--foreman-proxy-dns-managed=true \
--foreman-proxy-dns-provider=nsupdate_gss \
--foreman-proxy-dns-server="idm1.example.com" \
--foreman-proxy-dns-tsig-principal="capsule/satellite.example.com@EXAMPLE.COM" \
--foreman-proxy-dns-tsig-keytab=/etc/foreman-proxy/dns.keytab \
--foreman-proxy-dns-reverse="55.168.192.in-addr.arpa" \
--foreman-proxy-dns-zone=example.com \
--foreman-proxy-dns-ttl=86400
```

2. **重启 Satellite 或 Capsule 的 Proxy 服务。**

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

运行 satellite-installer 命令对胶囊配置进行任何更改后，您必须在卫星 Web UI 中更新每个受影响的胶囊的配置。

在卫星 Web UI 中更新配置

1. 导航到 Infrastructure > Capsules，找到 Satellite Server，然后从 Actions 列中的列表中，选择 Refresh。

2. 配置域：

   a. 导航到 Infrastructure > Domains 并选择域名。

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

3. 配置子网：

   a. 导航到 Infrastructure > Subnets 并选择子网名称。

   b. 在 子网 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 设置为连接子网的胶囊。

   e. 单击 Submit 以保存更改。

5.4.2. 使用 TSIG 身份验证配置动态 DNS 更新

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

前提条件

- 您必须确保部署 IdM 服务器，且正确配置了基于主机的防火墙。有关更多信息，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 服务器中获取 root 用户访问权限。

- 您必须确认卫星服务器或胶囊服务器是否已配置为为您的部署提供 DNS 服务。

- 您必须在管理部署的 DNS 服务 Satellite 或 Capsule 基础操作系统上配置 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 配置卫星服务器。

流程

要使用 TSIG 身份验证配置动态 DNS 更新，请完成以下步骤：

为 IdM 服务器中的 DNS 区启用外部更新

1. 在 IdM 服务器中，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 命名的 服务以使更改生效：

```
# systemctl reload named
```

3. 在 IdM web UI 中，进入 Network Services > 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。输入以下命令：**

```
# 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 指定组。通常，satellite-installer 可确保 foreman-proxy 用户属于指定的 UNIX 组，但是在这种情况下，卫星不管理用户和组，因此您需要将 foreman-proxy 用户手动分配给指定组。**

```
# usermod -a -G named foreman-proxy
```

7. **在 Satellite 服务器中，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=true \
--foreman-proxy-dns-managed=false \
--foreman-proxy-dns-provider=nsupdate \
--foreman-proxy-dns-server="IdM_Server_IP_Address" \
--foreman-proxy-keyfile=/etc/rndc.key \
--foreman-proxy-dns-ttl=86400
```

在 IdM 服务器中测试到 DNS 区的外部更新

1. 确保 Satellite Server 中的 /etc/rndc.key 文件中的键是 IdM 服务器中使用的相同密钥文件：

```
key "rndc-key" {
        algorithm hmac-md5;
        secret "secret-key==";
};
```

2. 在卫星服务器上，为主机创建测试 DNS 条目。例如，在位于 192.168.25.1 的 IdM 服务器上的 A 记录为 192.168.25.20 的主机 *test.example.com*。

```
# 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 服务器中测试 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，请导航至 Network Services > DNS > DNS Zones。单击区域的名称，再按名称搜索主机。

5. 如果成功解决，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. 确认删除了 DNS 条目：

```
# nslookup test.example.com 192.168.25.1
```

以上 nslookup 命令会失败，并在成功删除记录时返回 SERVFAIL 错误消息。

5.4.3. 恢复到内部 DNS 服务

您可以将 恢复为使用卫星服务器和胶囊服务器作为您的 DNS 提供程序。您可以使用在配置外部 DNS 之前创建的应答文件的备份，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 配置卫星服务器。

流程

在您要配置的 Satellite 或 Capsule 服务器中为域管理 DNS 服务，请完成以下步骤：

将卫星或胶囊配置为 DNS 服务器

- 如果您在配置外部 DNS 前创建了应答文件的备份，请恢复回答文件，然后输入 satellite-installer 命令：

```
# satellite-installer
```

- 如果您对应答文件有合适的备份，请现在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 上输入以下 satellite-installer 命令以及每个受影响的胶囊：

```
# satellite-installer \
--foreman-proxy-dns=true \
--foreman-proxy-dns-managed=true \
--foreman-proxy-dns-provider=nsupdate \
--foreman-proxy-dns-server="127.0.0.1"  \
--foreman-proxy-dns-tsig-principal="foremanproxy/satellite.example.com@EXAMPLE.COM" \
--foreman-proxy-dns-tsig-keytab=/etc/foreman-proxy/dns.keytab
```

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 命令对胶囊配置进行任何更改后，您必须在卫星 Web UI 中更新每个受影响的胶囊的配置。

在卫星 Web UI 中更新配置

1. 导航到 Infrastructure > Capsules。
2. 对于您要更新的每个胶囊，请从 Actions 列表中选择 Refresh。

3. **配置域：**

   a. 进入 **Infrastructure > Domains** 并点您要配置的域名。

   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. 导航到 **Infrastructure > Subnets** 并选择子网名称。

   b. 在 **Subnet** 选项卡中，将 **IPAM** 设置为 **DHCP** 或内部数据库。

   c. 在 **Domains** 选项卡中，选择您要使用卫星或胶囊管理的域。

   d. 在 **Capsules** 选项卡中，将 **Reverse DNS Capsule** 设置为连接子网的胶囊。

   e. 单击 **Submit** 以保存更改。

附录 A. 将自定义配置应用到 RED HAT SATELLITE

当您首次使用 satellite-installer 安装并配置 Satellite 时，您可以指定 DNS 和 DHCP 配置文件不是由 Puppet 使用安装程序标志 --foreman-proxy-dns-managed=false 和 --foreman-proxy-dhcp-managed=false 管理=false 进行管理的 DNS 和 DHCP 配置文件。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，重新运行 以便升级目的。如果更改被覆盖，则必须运行恢复过程来恢复手动更改。如需更多信息，请参阅"从 Puppet 运行"写入的手动更改。

要查看可用于自定义配置的所有安装程序标志，请运行 satellite-installer --scenario satellite --full-help。些 Puppet 类不暴露于卫星安装程序。要手动管理并阻止安装程序覆盖其值，请在配置文件 /etc/foreman-installer/custom-hiera.yaml 中添加条目来指定配置值。此配置文件采用 YAML 格式，以 < puppet class>::<parameter name>: <value> 的格式由每行一个条目组成。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
```

- 要完全关闭 Apache 服务器签名：

```
apache::server_signature: Off
```

卫星安装程序的 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 命令执行关键字搜索。

设置某些值可能会影响 Red Hat Satellite 的性能或功能时可能出现的后果。在应用前，请考虑更改的影响，然后首先在非生产环境中测试更改。如果您没有非生产环境，请使用 --noop 和 --verbose 选项运行 Satellite 安装程序。如果您的更改造成问题，请从 custom-hiera.yaml 中删除异常行，并重新运行 Satellite 安装程序。如果您对特定值是否安全修改，请联络红帽支持。

附录 B. 恢复由 PUPPET 运行编写的手动更改

如果 Puppet 运行覆盖了手动配置，您可以将文件恢复到之前的状态。以下示例演示了如何恢复由 Puppet 运行覆盖的 DHCP 配置文件。

流程

1. 复制要恢复的 文件。这可让您比较文件，以检查升级所需的任何强制更改。这不适用于 DNS 或 DHCP 服务。

```
# 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。