Red Hat Satellite 6.11

安装 Capsule 服务器

安装 Red Hat Satellite Capsule Server

Last Updated: 2024-02-15

Red Hat Satellite 6.11 安装 Capsule 服务器

安装 Red Hat Satellite Capsule Server

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

法律通告

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

摘要

本指南介绍了如何安装 Red Hat Satellite Capsule 服务器、执行初始配置以及配置外部服务。

目录

向红帽文档提供反馈 3

第 1 章 为安装准备您的环境 4
1.1. 系统要求 4
1.2. 存储要求 5
1.3. 存储指南 6
1.4. 支持的操作系统 7
1.5. 端口和防火墙要求 8
1.6. 启用从 CAPSULE 服务器到 SATELLITE 服务器的连接 11
1.7. 启用从 SATELLITE 服务器和客户端连接到 CAPSULE 服务器 12

第 2 章 安装 CAPSULE 服务器 13
2.1. 注册到 SATELLITE 服务器 13
2.2. 附加 SATELLITE 基础架构订阅 14
2.3. 配置软件仓库 16
2.4. 安装 CAPSULE 服务器软件包 17
2.5. 使用 CHRONYD 同步系统时钟 17
2.6. 使用 SSL 证书配置 CAPSULE 服务器 18
2.7. 在 SATELLITE WEB UI 中将修正的机构和位置分配给 CAPSULE 服务器 24

第 3 章 在 CAPSULE 服务器上执行其他配置 27
3.1. 配置 CAPSULE 以进行主机注册和置备 27
3.2. 在外部 CAPSULE 中启用 KATELLO 代理 28
3.3. 在 CAPSULE 服务器上启用 OPENSCAP 28
3.4. 将虚拟环境添加到 CAPSULE 服务器 28
3.5. 在受管主机上启用电源管理 30
3.6. 在 CAPSULE 服务器上配置 DNS、DHCP 和 TFTP 31

第 4 章 使用外部服务配置 CAPSULE 服务器 33
4.1. 使用外部 DNS 配置 CAPSULE 服务器 33
4.2. 使用外部 DHCP 配置 CAPSULE 服务器 34
4.3. 使用外部 TFTP 配置 CAPSULE 服务器 40
4.4. 使用外部 IDM DNS 配置 CAPSULE 服务器 41

第 5 章 使用 CAPSULE 管理 DHCP 52
5.1. 保护 DHCPD API 52

第 6 章 使用 CAPSULE 管理 DNS 54

附录 A. CAPSULE 服务器扩展注意事项 55

向红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。

您可以通过在 Bugzilla 中记录一个 ticket 来提交反馈：

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

第 1 章 为安装准备您的环境

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
- Red Hat Enterprise Linux 8 或 Red Hat Enterprise Linux 7 服务器的最新版本
- 至少 4 核 2.0 IANA CPU
- 胶囊式服务器至少需要 12 GB RAM。另外，还推荐最少使用 4 GB 的 swap 空间。运行的 RAM 少于最小值的 Capsule 可能无法正常工作。
- 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
- 系统 umask 为 0022
- 使用完全限定域名的全正向和反向 DNS 解析

Satellite 只支持 **UTF-8** 编码。如果您的要求是美国并且您的语言为英语，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，请参阅配置系统区域设置指南。

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。在使用自定义证书时，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 Capsule 服务器前，请确保您的环境满足安装要求。

警告

Capsule 的版本必须与安装的 Satellite 版本匹配。它不应该不同。例如，Capsule 版本 6.11 无法注册到 Satellite 版本 6.10。

除了运行 Capsule 服务器外，必须在提供其他功能的全新的调配系统上安装 Capsule 服务器。新置备的系统不得有外部身份提供程序提供的以下用户，以避免与 Capsule 服务器创建的本地用户冲突：

- Apache
- foreman-proxy
- postgres

- Pulp
- puppet
- qdrouterd
- redis

有关扩展 Capsule 服务器的更多信息，请参阅 Capsule 服务器扩展注意事项。

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 Capsule 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 Mode

必须启用 SELinux，可以是 enforcing 模式或 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 安全强化指南* 中的 安装启用了 FIPS 模式的 RHEL 8 系统。有关在 Red Hat Enterprise Linux 7 系统中 FIPS 的详情，请参考 *Red Hat Enterprise Linux 安全指南* 中的 启用 FIPS 模式。

注意

Satellite 支持 DEFAULT 和 FIPS 加密策略。Satellite 和 Capsule 安装不支持 FUTURE 加密策略。

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，并根据单个环境而有所不同。

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

Capsule 服务器上 PostgreSQL 数据库的大小可能会显著增加，同时增加从 Satellite 服务器同步的生命周期环境、内容视图或存储库的数量。在最大的 Satellite 环境中，胶囊服务器上的 PostgreSQL 目录的大小可以增加到 Satellite 服务器上的 PostgreSQL 目录大小的两倍或三倍。

1.2.1. Red Hat Enterprise Linux 8

表 1.1. Capsule 服务器安装的存储要求

目录	安装大小	运行时大小
/var/lib/pulp	1 MB	300 GB
/var/lib/pgsql	100 MB	20 GB
/usr	3 GB	不适用

目录	安装大小	运行时大小
/opt/puppetlabs	500 MB	不适用

1.2.2. Red Hat Enterprise Linux 7

表 1.2. Capsule 服务器安装的存储要求

目录	安装大小	运行时大小
/var/lib/pulp	1 MB	300 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

1.3. 存储指南

安装 Capsule 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，则必须在 **/etc/fstab** 文件中使用 **exec** 挂载选项。如果 **/tmp** 已使用 **noexec** 选项挂载，您必须将选项改为 **exec** 并重新挂载文件系统。这是 **puppetserver** 服务正常工作的要求。
- 因为大多数 Capsule 服务器数据存储在 **/var** 目录中，所以在 LVM 存储中挂载 **/var** 可以帮助系统扩展。
- **/var/lib/qpidd/** 目录在每个由 **goferd** 服务管理的内容主机使用大约 2 MB 以上。例如，10 000 内容主机需要 **/var/lib/qpidd/** 中的 20 GB 磁盘空间。
- 对 **/var/lib/pulp/** 目录使用高带宽、低延迟存储。由于 Red Hat Satellite 具有许多 I/O 密集型操作，因此使用高延迟，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** 脚本获取这些数据。有关使用 **storage-benchmark** 脚本的更多信息，请参阅 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 *Red* Hat Enterprise Linux 7 系统管理员指南中的日志轮转。

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
```

如果已经挂载了 NFS 共享，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存储一次在磁盘上。包含重复软件包的额外软件仓库需要较少的额外存储。存储批量位于 **/var/lib/pulp/** 目录中。这些端点不可手动配置。确保存储在 **/var** 文件系统中可用，以防止存储问题。

Software Collections

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

在安装到 **/opt** 目录时，需要 root 用户写入和执行权限。

符号链接

您不能将符号链接用于 **/var/lib/pulp/**。

同步 RHEL ISO

如果您计划将 RHEL 内容 ISO 与 Satellite 同步，请注意所有 Red Hat Enterprise Linux 次要版本也同步。您必须计划在 Satellite 上有足够的存储来管理此功能。

1.4. 支持的操作系统

您可以从红帽支持的磁盘、本地 ISO 镜像、Kickstart 或者任何其他方法安装操作系统。Red Hat Capsule Server 在 Red Hat Enterprise Linux 8 的最新版本上被支持，并在安装 Capsule 服务器时提供 Red Hat Enterprise Linux 7 服务器。不支持 Red Hat Enterprise Linux 的早期版本，包括 EUS 或 z-stream。

安装程序支持以下操作系统，有软件包，并已测试用于部署 Satellite：

表 1.3. satellite-installer 支持的操作系统

操作系统	架构	备注
Red Hat Enterprise Linux 8	仅 x86_64	
Red Hat Enterprise Linux 7	仅 x86_64	

在安装 Satellite 之前，请尽可能应用所有操作系统更新。

Red Hat Capsule Server 需要带有 **@Base** 软件包组的 Red Hat Enterprise Linux 安装，没有其他软件包组修改，不需要第三方配置或软件直接进行服务器操作。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，请先安装并验证完整的胶囊式服务器，然后先创建系统的备份，然后再添

加任何非红帽软件。

在全新调配的系统上安装 Capsule 服务器。

不要将 Capsule 服务器注册到 Red Hat Content Delivery Network (CDN)。

红帽不支持将系统用于运行 Capsule 服务器以外的任何内容。

1.5. 端口和防火墙要求

对于 Satellite 架构的组件进行通信，请确保在基础操作系统上打开所需的网络端口并空闲。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。

如果在安装启动前未打开 Satellite 服务器和 Capsule 服务器之间的端口，则安装 Capsule 服务器会失败。

使用此信息来配置任何基于网络的防火墙。请注意，有些虚拟化解决方案必须特别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，并在防火墙中知道。如果可能，禁用应用程序检查并允许根据协议打开端口通信。

集成的 Capsule

Satellite 服务器具有集成的 Capsule，并且任何直接连接到 Satellite 的主机都是本节上下文中 Satellite 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。

Capsule 的客户端

是 Satellite 集成胶囊之外的 Capsule 客户端的主机不需要访问 Satellite 服务器。有关 Satellite 拓扑的更多信息，*请参阅规划 Red Hat Satellite* 中的 Capsule 网络。

所需的端口可以根据您的配置而改变。

下表表示目标端口和网络流量方向：

表 1.4. Capsule 传入的流量

目的地端口	协议	服务	源	需要强制	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 Server （可选）	
443, 80	TCP	HTTPS, HTTP	客户端	内容检索	内容
443, 80	TCP	HTTPS, HTTP	客户端	内容主机注册	Capsule CA RPM 安装

目的地端口	协议	服务	源	需要强制	描述
443	TCP	HTTPS	Red Hat Satellite	内容镜像	管理
443	TCP	HTTPS	Red Hat Satellite	Capsule API	智能卡功能
443	TCP	HTTPS	客户端	内容主机注册	启动 上传事实 发送安装的软件包和追踪
5647	TCP	AMQP	客户端	Goferd 消息总线	将消息转发到客户端（可选） 与 Qpid 分配程序进行通信的 Katello 代理
8000	TCP	HTTP	客户端	置备模板	客户端安装程序、iPXE 或 UEFI HTTP 引导的模板检索
8000	TCP	HTTP	客户端	PXE 引导	安装
8140	TCP	HTTPS	客户端	Puppet 代理	客户端连接（可选）
8443	TCP	HTTPS	客户端	内容主机注册	在升级前部署的客户端主机已弃用且只需要
9090	TCP	HTTPS	客户端	注册端点	带有外部 Capsule 服务器的客户端注册
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	Capsule 功能

在此上下文中，任何直接连接到 Satellite 服务器的受管主机都是客户端，因为它是集成胶囊的客户端。这包括在其上运行 Capsule 服务器的基本操作系统。

DHCP Capsule 执行 ICMP ping 和 TCP 回显连接尝试到设置了 DHCP IPAM 的子网中的主机，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。

表 1.5. Capsule 传出流量

目的地端口	协议	服务	目的地	需要强制	描述
	ICMP	ping	客户端	DHCP	可用 IP 检查（可选）
7	TCP	echo	客户端	DHCP	可用 IP 检查（可选）
22	TCP	SSH	目标主机	远程执行	运行作业
53	TCP 和 UDP	DNS	Internet 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）
68	UDP	DHCP	客户端	动态 IP	DHCP （可选）
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	Red Hat Portal	SOS 报告	协助支持问题单（可选）
443	TCP	HTTPS	Satellite	内容	同步
443	TCP	HTTPS	Satellite	客户端通信	将来自客户端的请求转发到 Satellite
443	TCP	HTTPS	Infoblox DHCP 服务器	DHCP 管理	当将 Infoblox 用于 DHCP 时，管理 DHCP 租期（可选）
623			客户端	电源管理	BMC On/Off/Cycle/Status

目的地端口	协议	服务	目的地	需要强制	描述
5646	TCP	AMQP	Satellite Server	Katello 代理	将消息转发到 Capsule 上的 Qpid 分配路由器（可选）
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）

注意

ICMP 到端口 7 UDP 和 TCP 不能被拒绝，但可以被丢弃。DHCP Capsule 向客户端网络发送 ECHO REQUEST，以验证 IP 地址是否可用。任何响应都将阻止分配 IP 地址。

1.6. 启用从 CAPSULE 服务器到 SATELLITE 服务器的连接

在 Satellite 服务器上，您必须启用从 Capsule 服务器到 Satellite 服务器的传入连接，并使该规则在重启后保持不变。

先决条件

- 确保 Satellite 服务器上的防火墙规则被配置为为客户端与 Satellite 通信启用连接，因为 Capsule 服务器是 Satellite 服务器的客户端。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 启用 从客户端到 Satellite* 服务器的连接。

流程

1. 在 Satellite 服务器上，输入以下命令打开 Capsule 到 Satellite 通信的端口：

```
# firewall-cmd --add-port="5646/tcp"
```

2. 使更改持久：

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

1.7. 启用从 SATELLITE 服务器和客户端连接到 CAPSULE 服务器

在您要安装 Capsule 的基本操作系统上，您必须启用从 Satellite 服务器和客户端到 Capsule 服务器的传入连接，并使这些规则在重启后保持不变。

流程

1. 在您要在其上安装 Capsule 的基本操作系统中，输入以下命令打开 Satellite 服务器和客户端与 Capsule 服务器通信的端口：

```
# firewall-cmd \
--add-port="53/udp" --add-port="53/tcp" \
--add-port="67/udp" \
--add-port="69/udp" \
--add-port="80/tcp" --add-port="443/tcp" \
--add-port="5647/tcp" \
--add-port="8140/tcp" \
--add-port="8443/tcp" \
--add-port="8000/tcp" --add-port="9090/tcp"
```

2. 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 安全指南* 中的 使用和配置 firewalld，以及 *Red Hat Enterprise Linux 7 安全指南* 中的 firewalld 入门。

第 2 章 安装 CAPSULE 服务器

在安装 Capsule 服务器前，您必须确保您的环境满足安装要求。如需更多信息，请参阅为安装准备您的环境。

2.1. 注册到 SATELLITE 服务器

使用这个流程将您要在其上安装 Capsule 服务器的基本操作系统注册到 Satellite 服务器。

Red Hat Subscription Manifest 先决条件

- 在 Satellite 服务器上，必须安装清单，它必须包含您希望 Capsule 属于的组织的适当存储库。
- 清单必须包含您要在其上安装 Capsule 的基本操作系统的软件仓库，以及您要连接到 Capsule 的任何客户端。
- 存储库必须同步。

如需有关清单和存储库的更多信息，请参阅 *Red Hat Satellite 内容管理指南中的管理红帽订阅*。

代理和网络先决条件

- Satellite 服务器基础操作系统必须能够解析 Capsule 基础操作系统的主机名，反之亦然。
- 确保 Capsule 服务器和 Satellite 服务器之间可以使用客户端证书身份验证进行 HTTPS 连接。不支持 Capsule 服务器和 Satellite 服务器之间的 HTTP 代理。
- 您必须相应地配置主机和基于网络的防火墙。如需更多信息，请参阅 端口和防火墙要求。您可以使用主机注册功能、Satellite API 或hammer CLI 将主机注册到 Satellite。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > Register Host**。
2. 点 **Generate** 来创建注册命令。
3. 点 *文件* 图标将命令复制到您的剪贴板中。
4. 登录到您要注册并运行之前生成的命令的主机。
5. 检查 **/etc/yum.repos.d/redhat.repo** 文件，并确保已启用适当的存储库。

CLI 过程

1. 使用hammer CLI 生成主机注册命令：

```
# hammer host-registration generate-command \
--activation-keys "My_Activation_Key"
```

如果您的主机不信任 Satellite 服务器的 SSL 证书，您可以通过在注册命令中添加 **--insecure** 标志来禁用 SSL 验证。

```
# hammer host-registration generate-command \
--activation-keys "My_Activation_Key" \
--insecure true
```

2. 登录到您要注册并运行之前生成的命令的主机。
3. 检查 **/etc/yum.repos.d/redhat.repo** 文件，并确保已启用适当的存储库。

API 流程

1. 使用 Satellite API 生成主机注册命令：

```
# curl -X POST https://satellite.example.com/api/registration_commands \
--user "My_User_Name" \
-H 'Content-Type: application/json' \
-d '{ "registration_command": { "activation_keys": ["My_Activation_Key_1,
My_Activation_Key_2"] }}'
```

如果您的主机不信任 Satellite 服务器的 SSL 证书，您可以通过在注册命令中添加 **--insecure** 标志来禁用 SSL 验证。

```
# curl -X POST https://satellite.example.com/api/registration_commands \
--user "My_User_Name" \
-H 'Content-Type: application/json' \
-d '{ "registration_command": { "activation_keys": ["My_Activation_Key_1,
My_Activation_Key_2"], "insecure": true }}'
```

使用激活码简化指定环境。如需更多信息，请参阅 *内容管理指南中的管理激活码*。

要以命令行参数形式输入密码，请使用 **username:password** 语法。请记住，这会在 shell 历史记录中保存密码。

有关注册的更多信息，请参阅 *管理主机* 中的 将主机注册到 Red Hat Satellite 。

2. 登录到您要注册并运行之前生成的命令的主机。
3. 检查 **/etc/yum.repos.d/redhat.repo** 文件，并确保已启用适当的存储库。

2.2. 附加 SATELLITE 基础架构订阅

注意

如果您在 Satellite 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 Capsule 服务器。有关 SCA 的更多信息，请参阅 简单内容访问。

注册了 Capsule 服务器后，您必须识别您的订阅池 ID 并附加可用的订阅。Red Hat Satellite Infrastructure 订阅提供对 Red Hat Satellite 和 Red Hat Enterprise Linux 内容的访问。对于 Red Hat Enterprise Linux 7，它还提供对 Red Hat Software Collections (RHSCL)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 Infrastructure Subscriptions MCT3718 MCT3719 。

如果订阅还没有附加到系统，则会将其归类为 available。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 如何找出哪些订阅已被 Red Hat Subscription Manager 注册的客户端使用？ 以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 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 订阅附加到您的 Capsule 服务器运行的基本操作系统。如果在 Satellite 服务器上启用了 SCA，您可以跳过这一步：

```
# 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 Satellite Infrastructure 订阅是否已附加：

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

2.3. 配置软件仓库

使用这个流程启用安装 Capsule 服务器所需的存储库。选择您要在其中安装的操作系统和版本对应的选项：

- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 7

2.3.1. Red Hat Enterprise Linux 8

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-capsule-6.11-for-rhel-8-x86_64-rpms \
--enable=satellite-maintenance-6.11-for-rhel-8-x86_64-rpms
```

3. 启用模块：

```
# dnf module enable satellite-capsule: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** 依赖于模块 **postgresql:12** 和 **ruby:2.7**，该模块将使用 **satellite:el8** 模块启用。这些警告不会导致安装过程失败，因此可以安全地忽略。有关 Red Hat Enterprise Linux 8 中的模块和生命周期流的更多信息，请参阅 Red Hat Enterprise Linux Application Streams 生命周期。

2.3.2. 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-capsule-6.11-rpms \
--enable=rhel-7-server-satellite-maintenance-6.11-rpms \
--enable=rhel-server-rhscl-7-rpms \
--enable=rhel-7-server-ansible-2.9-rpms
```

注意

如果要将 Capsule 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 Red Hat Enterprise Linux 上安装客户机代理和驱动程序。

3. 清除任何元数据：

```
# yum clean all
```

4. 可选：验证是否启用了所需的存储库：

```
# yum repolist enabled
```

2.4. 安装 CAPSULE 服务器软件包

在安装胶囊式服务器软件包前，您必须更新安装在基本操作系统上的所有软件包。

- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8

流程

要安装 Capsule 服务器，请完成以下步骤：

2.4.1. Red Hat Enterprise Linux 7

1. 更新所有软件包：

```
# yum update
```

2. 安装 Satellite 服务器软件包：

```
# yum install satellite-capsule
```

2.4.2. Red Hat Enterprise Linux 8

1. 更新所有软件包：

```
# yum update
```

2. 安装 Satellite 服务器软件包：

```
# dnf install satellite-capsule
```

2.5. 使用 CHRONYD 同步系统时钟

要最大程度降低时间偏移的影响，您必须在要在其上使用网络时间协议(NTP)服务器安装胶囊式服务器的基本操作系统上同步系统时钟。如果正确配置了基础操作系统时钟，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，以及 Red Hat Enterprise Linux 7 系统管理员指南中的 使用 chrony 套件配置 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
```

2.6. 使用 SSL 证书配置 CAPSULE 服务器

Red Hat Satellite 使用 SSL 证书来启用 Satellite 服务器、外部 Capsule 服务器和所有主机之间的加密通信。根据机构的要求，您必须使用默认或自定义证书配置您的 Capsule 服务器。

- 如果您使用默认 SSL 证书，还必须使用不同的默认 SSL 证书配置每个外部 Capsule 服务器。更多信息请参阅 第 2.6.1 节 "使用默认 SSL 证书配置 Capsule 服务器"。
- 如果您使用自定义 SSL 证书，还必须使用不同的自定义 SSL 证书配置每个外部 Capsule 服务器。更多信息请参阅 第 2.6.2 节 "使用自定义 SSL 证书配置 Capsule 服务器"。

2.6.1. 使用默认 SSL 证书配置 Capsule 服务器

使用本节配置由 Satellite 服务器默认证书颁发机构(CA)签名的 SSL 证书的 Capsule 服务器。

先决条件

- Capsule 服务器已注册到 Satellite 服务器。如需更多信息，请参阅 注册到 Satellite 服务器。
- 已安装 Capsule 服务器软件包。如需更多信息，请参阅安装 Capsule 服务器软件包。

流程

1. 在 Satellite 服务器上，要为您的胶囊服务器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，如 **/root/capsule_cert** ：

```
# mkdir /root/capsule_cert
```

2. 在 Satellite 服务器上，为您的 Capsule 服务器生成 **/root/capsule_cert/prompt.example.com-certs.tar** 证书存档：

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

保留 **satellite-installer** 命令的副本，该命令会返回该副本，以将证书部署到您的 Capsule 服务器。

evince -certs-generate 的输出示例

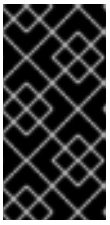
```
output omitted
satellite-installer --scenario capsule \
--certs-tar-file "/root/capsule_cert/capsule.example.com-certs.tar" \
--foreman-proxy-register-in-foreman "true" \
--foreman-proxy-foreman-base-url "https://satellite.example.com" \
--foreman-proxy-trusted-hosts "satellite.example.com" \
--foreman-proxy-trusted-hosts "capsule.example.com" \
--foreman-proxy-oauth-consumer-key "s97QxvUAgFNAQZNGg4F9zLq2biDsxM7f" \
--foreman-proxy-oauth-consumer-secret "6bpzAdMpRAfYaVZtaepYetomgBVQ6ehY"
```

3. 在 Satellite 服务器上，将证书归档文件复制到您的 Capsule 服务器中：

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

4. 在 Capsule 服务器上，要部署证书，请输入其 satellite- certs-generate 命令返回的 satellite- installer 命令。

当 Satellite 的网络连接或端口还没有打开时，您可以将 --foreman-proxy-register-in-foreman 选项设置为 false，以防止 Capsule 尝试连接到 Satellite 并报告错误。当正确配置了网络和防火墙时，将此选项设置为 true 再次运行安装程序。



重要

在部署证书后，请勿删除证书存档文件。例如，在升级 Capsule 服务器时需要这样做。

2.6.2. 使用自定义 SSL 证书配置 Capsule 服务器

如果您将 Satellite 服务器配置为使用自定义 SSL 证书，还必须使用不同的自定义 SSL 证书配置每个外部 Capsule 服务器。

要使用自定义证书配置您的 Capsule 服务器，请在每个 Capsule 服务器上完成以下步骤：

1. 第 2.6.2.1 节 “为 Capsule 服务器创建自定义 SSL 证书”

2. 第 2.6.2.2 节 “将自定义 SSL 证书部署到 Capsule 服务器”

3. 第 2.6.2.3 节 “将自定义 SSL 证书部署到主机”

2.6.2.1. 为 Capsule 服务器创建自定义 SSL 证书

在受管主机上，为您的胶囊服务器创建一个自定义证书。如果您已经为 Capsule 服务器有自定义 SSL 证书，请跳过这个过程。

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/capsule_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。

   如果您已有此胶囊服务器的私钥，请跳过这一步。

```
# openssl genrsa -out /root/capsule_cert/capsule_cert_key.pem 4096
```

3. 为 CSR 创建 /root/capsule_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 ]
CN = capsule.example.com

[ 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 = capsule.example.com
```

4. **生成 CSR：**

```
# openssl req -new \
-key /root/capsule_cert/capsule_cert_key.pem \ 1
-config /root/capsule_cert/openssl.cnf \ 2
-out /root/capsule_cert/capsule_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。**

5. **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。

2.6.2.2. 将自定义 SSL 证书部署到 Capsule 服务器

使用这个流程，使用证书颁发机构签名的自定义 SSL 证书配置您的 Capsule 服务器。satellite-installer 命令，其 return-certs-generate 命令为每个 Capsule 服务器是唯一的。不要在多个胶囊服务器

上使用相同的命令。

先决条件

- Satellite 服务器配置了自定义证书。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 使用自定义 SSL 证书配置 Satellite 服务器。
- Capsule 服务器已注册到 Satellite 服务器。如需更多信息，请参阅 注册到 Satellite 服务器。
- 已安装 Capsule 服务器软件包。如需更多信息，请参阅安装 Capsule 服务器软件包。

流程

1. 在 Satellite 服务器上，验证自定义 SSL 证书输入文件：

```
# katello-certs-check \
-t capsule -c /root/capsule_cert/capsule_cert.pem \ 1
-k /root/capsule_cert/capsule_cert_key.pem \ 2
-b /root/capsule_cert/ca_cert_bundle.pem 3
```

1. 由证书颁发机构签名的 Capsule 服务器证书文件的路径。
2. 用于为 Capsule 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。

如果您在 /root/capsule_cert/openssl.cnf 配置文件中为证书的 Common Name CN = 设置通配符值，您必须在 katello -certs-check 命令中添加 -t \":\" 选项。

如果命令成功，它会返回两个 evince -certs-generate 命令，则必须使用其中一个命令为您的 Capsule 服务器生成证书文件。

katello-certs-check的输出示例

```
Validation succeeded.

To use them inside a NEW $CAPSULE, run this command:

capsule-certs-generate --foreman-proxy-fqdn "$CAPSULE" \
    --certs-tar  "~/$CAPSULE-certs.tar" \
    --server-cert "/root/capsule_cert/capsule_cert.pem" \
    --server-key "/root/capsule_cert/capsule_cert_key.pem" \
    --server-ca-cert "/root/capsule_cert/ca_cert_bundle.pem" \

To use them inside an EXISTING $CAPSULE, run this command INSTEAD:

  capsule-certs-generate --foreman-proxy-fqdn "$CAPSULE" \
    --certs-tar "~/$CAPSULE-certs.tar" \
    --server-cert "/root/capsule_cert/capsule_cert.pem" \
    --server-key "/root/capsule_cert/capsule_cert_key.pem" \
    --server-ca-cert "/root/capsule_cert/ca_cert_bundle.pem" \
    --certs-update-server
```

2. **在 Satellite 服务器上，从 katello-certs-check 命令的输出中，根据您的要求，输入为新或现有 Capsule 生成证书的 evince -certs-generate 命令。**

   在此命令中，将 $CAPSULE 更改为您的 Capsule 服务器的 FQDN。

3. **保留 satellite-installer 命令的副本，该命令会返回该副本，以将证书部署到您的 Capsule 服务器。**

evince -certs-generate 的输出示例

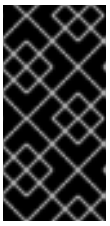
```
output omitted
satellite-installer --scenario capsule \
--certs-tar-file "/root/capsule.example.com-certs.tar" \
--foreman-proxy-register-in-foreman "true" \
--foreman-proxy-foreman-base-url "https://satellite.example.com" \
--foreman-proxy-trusted-hosts "satellite.example.com" \
--foreman-proxy-trusted-hosts "capsule.example.com" \
--foreman-proxy-oauth-consumer-key "s97QxvUAgFNAQZNGg4F9zLq2biDsxM7f" \
--foreman-proxy-oauth-consumer-secret "6bpzAdMpRAfYaVZtaepYetomgBVQ6ehY"
```

4. 在 Satellite 服务器上，将证书归档文件复制到您的 Capsule 服务器中：

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

5. 在 Capsule 服务器上，要部署证书，请输入其 satellite- certs-generate 命令返回的 satellite- installer 命令。

当 Satellite 的网络连接或端口还没有打开时，您可以将 --foreman-proxy-register-in-foreman 选项设置为 false，以防止 Capsule 尝试连接到 Satellite 并报告错误。当正确配置了网络和防火墙时，将此选项设置为 true 再次运行安装程序。



重要

在部署证书后，请勿删除证书存档文件。例如，在升级 Capsule 服务器时需要这样做。

2.6.2.3. 将自定义 SSL 证书部署到主机

将 Capsule 服务器配置为使用自定义 SSL 证书后，还必须在注册到此 Capsule 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://capsule.example.com/pub/katello-ca-consumer-latest.noarch.rpm
```

2.7. 在 SATELLITE WEB UI 中将修正的机构和位置分配给 CAPSULE 服务器

安装 Capsule 服务器软件包后，如果有多个机构或位置，则必须为 Capsule 分配正确的机构和位置，以便在 Satellite Web UI 中可见 Capsule。

注意

将 Capsule 分配给与带有嵌入式 Capsule 的 Satellite 服务器相同的位置，可防止 Red Hat Insights 上传 Insights 清单。若要启用清单上传，请为这两个胶囊同步 SSH 密钥。

流程

1. *登录 Satellite Web UI。*
2. *从屏幕左上角的 Organization 列表中选择 任何机构。*
3. *从屏幕左上角的 Location 列表中，选择 Any Location。*
4. *在 Satellite Web UI 中，导航到 Hosts > All Hosts 并选择 Capsule Server。*
5. *从 Select Actions 列表中，选择 Assign Organization。*
6. *从 Organization 列表中，选择要分配此 Capsule 的组织。*
7. *点 Mismatch 上的 Fix Organization。*
8. *点 Submit。*
9. *选择胶囊式服务器。从 Select Actions 列表中，选择 Assign Location。*
10. *从 Location 列表中，选择您要分配此 Capsule 的位置。*
11. *点 Mismatch 上的 Fix Location。*
12. *点 Submit。*

13. 在 Satellite Web UI 中，导航到 Administer > Organizations，再点击您为其分配 Capsule 的组织。

14. 单击 Capsules 选项卡，并确保在 Selected items 列表下列出 Capsule 服务器，然后单击 Submit。

15. 在 Satellite Web UI 中，导航到 Administer > Locations，然后点击您为其分配 Capsule 的位置。

16. 单击 Capsules 选项卡，并确保在 Selected items 列表下列出 Capsule 服务器，然后单击 Submit。

验证

（可选）您可以验证 Satellite Web UI 中是否已正确列出 Capsule 服务器。

1. 从 Organization 列表中选择机构。

2. 从 Location 列表中选择位置。

3. 在 Satellite Web UI 中，导航到 Hosts > All Hosts。

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

第 3 章 在 CAPSULE 服务器上执行其他配置

使用本章在 Capsule 服务器上配置其他设置。

3.1. 配置 CAPSULE 以进行主机注册和置备

使用这个流程配置 Capsule，以便您可以使用 Capsule 服务器而不是 Satellite 服务器注册和置备主机。

流程

- 在命令行中，将胶囊添加到可信代理列表中。

  Satellite 需要此项来识别通过 Capsule 设定的 X-Forwarded-For HTTP 标头转发的主机 IP 地址。为安全起见，Satellite 默认仅识别来自 localhost 的这个 HTTP 标头。您可以输入可信代理作为有效的 IPv4 或 Capsules 的 IPv6 地址或网络范围。

  警告

  不要使用过大的网络范围，因为这可能会造成潜在的安全风险。

  输入以下命令。请注意，命令会覆盖当前存储在 Satellite 中的列表。因此，如果您之前设置了任何可信代理，则必须将它们包含在命令中：

```
# satellite-installer \
--foreman-trusted-proxies "127.0.0.1/8" \
--foreman-trusted-proxies "::1" \
--foreman-trusted-proxies "My_IP_address" \
--foreman-trusted-proxies "My_IP_range"
```

  localhost 条目是必需的，不要省略它们。

验证

1. 使用 Satellite 安装程序的完整帮助列出当前可信代理：

```
# satellite-installer --full-help | grep -A 2 "trusted-proxies"
```

2. 当前列表包含您需要的所有可信代理。

3.2. 在外部 CAPSULE 中启用 KATELLO 代理

远程执行是在内容主机上管理软件包的主要方法。为了可以使用已弃用的 Katello 代理，必须在每个 Capsule 上启用它。

流程

- 要启用 Katello Agent 基础架构，请输入以下命令：

```
# satellite-installer --scenario capsule \
--foreman-proxy-content-enable-katello-agent=true
```

3.3. 在 CAPSULE 服务器上启用 OPENSCAP

在 Satellite 服务器和 Satellite 服务器的集成胶囊上，OpenSCAP 被默认启用。要在外部胶囊上使用 OpenSCAP 插件和内容，您必须在每个胶囊上启用 OpenSCAP。

流程

- 要启用 OpenSCAP，请输入以下命令：

```
# satellite-installer --scenario capsule \
--enable-foreman-proxy-plugin-openscap \
--foreman-proxy-plugin-openscap-puppet-module true
```

如果要使用 Puppet 部署合规策略，您必须首先启用它。如需更多信息，请参阅在 Red Hat Satellite 中使用 Puppet 集成管理配置。

3.4. 将虚拟环境添加到 CAPSULE 服务器

如果您的 Capsule 服务器启用了内容功能，您必须添加一个环境，以便 Capsule 可以从 Satellite 服务器同步内容，并将内容提供给主机系统。

不要将 库虚拟化环境 分配给您的 Capsule 服务器，因为它在每次 CDN 更新存储库时触发自动 Capsule 同步。这可能会在 Capsule 上消耗多个系统资源、Satellite 和 Capsule 之间的网络带宽，以及胶囊上的可用磁盘空间。

您可以在 Satellite 服务器或 Satellite Web UI 上使用hammer CLI。

流程

1. 在 Satellite Web UI 中，导航到 Infrastructure > Capsules，然后选择您要向其添加生命周期的 Capsule。
2. 点 Edit 并点 Life Cycle Environments 选项卡。
3. 在左侧菜单中选择您要添加到 Capsule 的生命周期阶段，然后单击 Submit。
4. 若要同步 Capsule 上的内容，请单击 Overview 选项卡，然后单击 同步。
5. 选择 Optimized Sync 或 Complete Sync。

   有关每种同步类型的定义，请参阅恢复仓库。

CLI 过程

1. 要显示所有 Capsule 服务器的列表，在 Satellite 服务器上输入以下命令：

   ```
   # hammer capsule list
   ```

   请注意您要向其添加生命周期的 Capsule 的 Capsule ID。
2. 使用 ID，验证您的 Capsule 的详情：

   ```
   # hammer capsule info --id capsule_id
   ```

3. 要查看您的 Capsule 服务器可用的生命周期阶段，请输入以下命令并记录 ID 和机构名称：

```
# hammer capsule content available-lifecycle-environments --id capsule_id
```

4. 将生命周期阶段添加到您的 Capsule 服务器中：

```
# hammer capsule content add-lifecycle-environment \
--id capsule_id --organization "My_Organization" \
--lifecycle-environment-id lifecycle-environment_id
```

对您要添加到 Capsule 服务器的每个生命周期环境重复此操作。

5. 将内容从 Satellite 同步到 Capsule。

- 要将 Satellite 服务器环境中的所有内容同步到 Capsule 服务器，请输入以下命令：

```
# hammer capsule content synchronize --id capsule_id
```

- 要将特定生命周期环境从 Satellite 服务器同步到 Capsule 服务器，请输入以下命令：

```
# hammer capsule content synchronize --id external_capsule_id \
--lifecycle-environment-id lifecycle-environment_id
```

3.5. 在受管主机上启用电源管理

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

先决条件

- 所有受管主机都必须有一个 BMC 类型的网络接口。Capsule 服务器使用此 NIC 将适当的凭证传递给主机。如需更多信息，请参阅 管理主机 指南中的 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 --scenario capsule \
--foreman-proxy-bmc "true" \
--foreman-proxy-bmc-default-provider "freeipmi"
```

3.6. 在 CAPSULE 服务器上配置 DNS、DHCP 和 TFTP

要在 Capsule 服务器上配置 DNS、DHCP 和 TFTP 服务，请使用 satellite-installer 命令和适合您的环境的选项。要查看可配置选项的完整列表，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时。

要使用外部 DNS、DHCP 和 TFTP 服务，请参阅 第 4 章 使用外部服务配置 Capsule 服务器。

添加多宿 DHCP 详情

如果要使用 Multihomed DHCP，您必须通知安装程序。

先决条件

- 您必须有 DNS 服务器的正确网络名称(dns-interface)。
- 您必须有 DHCP 服务器的正确接口名称(dhcp-interface)。
- 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。以下示例演示了配置完整的置备服务：

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

有关配置 DHCP、DNS 和 TFTP 服务的更多信息，请参阅置备指南中的配置网络服务。https://access.redhat.com/documentation/zh-cn/red_hat_satellite/6.11/html-single/provisioning_hosts/index#Configuring_Network_Services_provisioning

第 4 章 使用外部服务配置 CAPSULE 服务器

如果您不想在 Capsule 服务器上配置 DNS、DHCP 和 TFTP 服务，请使用本节将 Capsule 服务器配置为与外部 DNS、DHCP 和 TFTP 服务一起工作。

4.1. 使用外部 DNS 配置 CAPSULE 服务器

您可以使用外部 DNS 配置 Capsule 服务器。Capsule 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，您必须输入 satellite-installer 命令以及适合您的环境的选项。

先决条件

- 您必须已配置了外部 DNS 服务器。
- 本指南假设您已有安装。

流程

1. 将 /etc/rndc.key 文件从外部 DNS 服务器复制到 Capsule 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，导航到 **Infrastructure > Capsules**。

6. 找到 **Capsule** 服务器，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。

4.2. 使用外部 DHCP 配置 CAPSULE 服务器

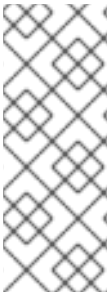
要使用外部 **DHCP** 配置 **Capsule** 服务器，您必须完成以下步骤：

1. 第 4.2.1 节 “配置外部 DHCP 服务器以用于 Capsule 服务器”

2. 第 4.2.2 节 “使用外部 DHCP 服务器配置 Satellite 服务器”

4.2.1. 配置外部 DHCP 服务器以用于 Capsule 服务器

要将运行 **Red Hat Enterprise Linux** 的外部 **DHCP** 服务器配置为与 **Capsule** 服务器搭配使用，您必须安装 **ISC DHCP Service** 和 **Berkeley Internet Name Domain (BIND)**或其实用程序软件包。您还必须与 **Capsule** 服务器共享 **DHCP** 配置和租期文件。此流程中的示例使用分布式网络文件系统**(NFS)**协议来共享 **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 grub2/ 子目录下在 TFTP 服务器上创建配置文件。如果禁用了 dhcp-no-override 设置，客户端会从根目录中获取引导装载程序及其配置，这可能会导致错误。

流程

1. 在您的 Red Hat Enterprise Linux 主机上，根据您的主机版本安装 ISC DHCP Service 和 BIND 软件包。

   - 对于 Red Hat Enterprise Linux 7 主机：

     ```
     # yum install dhcp bind
     ```

   - 对于 Red Hat Enterprise Linux 8 主机：

     ```
     # yum 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，当前目录中会创建一个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 "jNSE5YI3H1A8Oj/tkV4...A2ZOHb6zv315CkNAY7DMYYCj48Umw==";
};
omapi-key omapi_key;
```

*请注意，**options router** 值是您要与外部 **DHCP** 服务一起使用的 **Satellite** 或 **Capsule IP** 地址。*

5. *从在其中创建的目录中删除两个密钥文件。*

6. *在 **Satellite** 服务器上，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，如果租期范围为 **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** 到 **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 \
&& firewall-cmd --runtime-to-permanent
```

8. *在 **Satellite** 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. 要确保配置文件可以访问，请恢复 **read** 和 **execute** 标记：

```
# 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 地址是要用于外部 DHCP 服务的 Satellite 或 Capsule IP 地址。

17. 重新载入 NFS 服务器：

```
# exportfs -rva
```

18. 为 DHCP omapi 端口 7911 配置防火墙：

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

19. 可选：配置防火墙以从外部访问 NFS。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
```

4.2.2. 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 Capsule 服务器。

前提条件

- 确保您已配置了外部 DHCP 服务器，并且您已与 Capsule 服务器共享 DHCP 配置和租期文件。更多信息请参阅 第 4.2.1 节 “配置外部 DHCP 服务器以用于 Capsule 服务器”。

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

11. 找到 Capsule 服务器，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。

4.3. 使用外部 TFTP 配置 CAPSULE 服务器

您可以使用外部 TFTP 服务配置 Capsule 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=true \
--foreman-proxy-tftp-root /mnt/nfs/var/lib/tftpboot
```

5. 如果 TFTP 服务在 DHCP 服务不同的服务器上运行，请使用 TFTP 服务在其中运行的服务器的 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，导航到 Infrastructure > Capsules。

7. 找到 Capsule 服务器，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。

4.4. 使用外部 IDM DNS 配置 CAPSULE 服务器

当 Satellite 服务器为主机添加 DNS 记录时，首先确定哪个 Capsule 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 Capsule 通信并添加记录。此过程中不涉及该主机。因此，您必须在 Satellite 或 Capsule 上安装和配置 IdM 客户端，该客户端当前配置为为您要使用 IdM 服务器管理的域提供 DNS 服务。

Capsule 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 Capsule 服务器配置为使用红帽身份管理(IdM)服务器来提供 DNS 服务，请使用以下流程之一：

- 第 4.4.1 节 “使用 GSS-TSIG 身份验证配置动态 DNS 更新”
- 第 4.4.2 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 4.4.3 节 “恢复到内部 DNS 服务”

注意

您不需要使用 Capsule 服务器来管理 DNS。当您使用 Satellite 的域注册功能时，置备的主机会自动注册到 IdM，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 Capsule 服务器是互斥的。有关配置域注册的更多信息，请参阅管理 Red Hat Satellite 指南中的置备主机 的 外部身份验证。

4.4.1. 使用 GSS-TSIG 身份验证配置动态 DNS 更新

您可以将 IdM 服务器配置为将通用安全服务算法用于 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 Capsule 服务器基础操作系统上安装 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 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，并有权在 IdM 服务器上创建区域。
- 您应该创建回答文件的备份。如果回答文件损坏，您可以使用备份将其恢复到其原始状态。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 服务器上创建 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 Capsule 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.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 的基本操作系统中，安装 ipa-client 软件包：

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

2. 运行安装脚本并遵循屏幕提示来配置 IdM 客户端：

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

3. 获取Kerberos ticket：

```
# kinit admin
```

4. 删除任何已存在的 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

将 keytab 添加到与服务原始系统相同的主机名的备用系统中时，添加 r 选项以防止生成新凭证并在原始系统上呈现凭据无效。

6. 对于 dns.keytab 文件，将所有者和组设置为 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：*

   a. *进入 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，在 BIND 更新策略 框中，将以下内容添加到分号分开的列表中：*

   ```
   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. *进入 Network Services > DNS > DNS Zones。*

   b. *点击 Add。*

   c. *选择 Reverse zone IP network 并使用 CIDR 格式添加网络地址来启用反向查找。*

   d. *点 Add and Edit。*

e. 点 Settings 选项卡，在 BIND 更新策略 框中，将以下内容添加到分号分开的列表中：

```
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 中输入以下命令：

```
satellite-installer --scenario satellite \
--foreman-proxy-dns=true \
--foreman-proxy-dns-managed=false \
--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
```

- 在 Capsule 中输入以下命令：

```
satellite-installer --scenario capsule \
--foreman-proxy-dns=true \
--foreman-proxy-dns-managed=false \
--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
```

运行 satellite-installer 命令对 Capsule 配置进行任何更改后，您必须在 Satellite Web UI 中更新每个受影响的 Capsule 的配置。

在 Satellite Web UI 中更新配置

1. 在 Satellite Web UI 中，导航到 Infrastructure > Capsules，找到 Capsule Server，并从 Actions 列中的列表，选择 Refresh。

2. 配置域：

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

   b. 在 Domain 选项卡中，确保将 DNS Capsule 设置为子网连接的 Capsule。

3. 配置子网：

   a. 在 Satellite Web UI 中，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，确保将 Reverse DNS Capsule 设置为子网连接的 Capsule。

   e. 点 Submit 保存更改。

4.4.2. 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 密钥文件的 DNS (TSIG)技术进行 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。
- 您必须在管理部署的 DNS 服务的 Satellite 或 Capsule 的基础操作系统上配置 DNS、DHCP 和 TFTP 服务。
- 您必须创建回答文件的备份。如果回答文件损坏，您可以使用备份将其恢复到其原始状态。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，导航到 Network Services > DNS > DNS Zones，然后点击区的名称。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=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
```

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 服务器中使用的密钥文件相同：

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

2. 在 Satellite 服务器上，为主机创建一个测试 DNS 条目。例如，在 192.168.25.1 的 IdM 服务

器上的 A 记录 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. 要查看 IdM Web UI 中的条目，请导航到 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 test 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，并在成功删除记录时返回 SERVFAIL 错误消息。

4.4.3. 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 之前创建的回答文件的备份，或者您可以创建回答文件的备份。有关回答文件的更多信息，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 前创建了回答文件的备份，请恢复回答文件，然后输入 satellite-installer 命令：*

```
# satellite-installer
```

- *如果您没有回答文件的合适的备份，请立即创建回答文件的备份。要在不使用回答文件的情况下将 Satellite 或 Capsule 配置为 DNS 服务器，请在 Satellite 或 Capsule 中输入以下 satellite-installer 命令：*

```
# satellite-installer \
--foreman-proxy-dns=true \
--foreman-proxy-dns-managed=true \
--foreman-proxy-dns-provider=nsupdate \
--foreman-proxy-dns-server="127.0.0.1"
```

如需更多信息，请参阅 Capsule 服务器上配置 DNS、DHCP 和 TFTP。

运行 satellite-installer 命令对 Capsule 配置进行任何更改后，您必须在 Satellite Web UI 中更新每个受影响的 Capsule 的配置。

在 Satellite Web UI 中更新配置

1. *在 Satellite Web UI 中，导航到 Infrastructure > Capsules。*
2. *对于您要更新的每个 Capsule，请从 Actions 列表中选择 Refresh。*
3. *配置域：*
   a. *在 Satellite Web UI 中，导航到 Infrastructure > Domains，然后点击您要配置的域名。*
   b. *在 Domain 选项卡中，将 DNS Capsule 设置为子网连接的 Capsule。*
4. *配置子网：*

a. 在 Satellite Web UI 中，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 DHCP 或 内部 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 设置为子网连接的 Capsule。

e. 点 Submit 保存更改。

第 5 章 使用 CAPSULE 管理 DHCP

Satellite 可以使用您的胶囊与 DHCP 服务集成。Capsule 具有多个 DHCP 提供程序，可用于将 Satellite 与现有 DHCP 基础架构集成或部署新的 DHCP 基础架构。您可以使用 Capsule 的 DHCP 模块来查询可用的 IP 地址、添加新和删除现有的保留。请注意，您的 Capsule 无法管理 subnet 声明。

可用的 DHCP 提供商

- dhcp_infoblox - 如需更多信息，请参阅 置备主机 中的 使用 Infoblox 作为 DHCP 和 DNS 提供商。
- dhcp_isc - OMAPI 的 ISC DHCP 服务器。如需更多信息，请参阅 安装 Capsule 服务器 中的 在 Capsule 服务器上配置 DNS、DHCP 和 TFTP。
- dhcp_remote_isc - 通过 OMAPI 进行 ISC DHCP 服务器，并通过网络挂载的租期。如需更多信息，请参阅 安装 Capsule 服务器 中的 配置外部 DHCP 服务器以与 Capsule 服务器 一起使用。

5.1. 保护 DHCPD API

Capsule 使用 dhcpd API 与 DHCP 守护进程交互来管理 DHCP。默认情况下，dhcpd API 侦听任何主机而不进行访问控制。您可以添加 omapi_key 以提供基本安全性。

流程

1. 安装所需的软件包：

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

2. 生成一个密钥：

```
# dnssec-keygen -r /dev/urandom -a HMAC-MD5 -b 512 -n HOST omapi_key
# cat Komapi_key.+*.private | grep ^Key|cut -d ' ' -f2-
```

3. 使用 satellite-installer 来保护 dhcpd API：

```
# satellite-installer \
--foreman-proxy-dhcp-key-name "My_Name" \
--foreman-proxy-dhcp-key-secret "My_Secret"
```

第 6 章 使用 CAPSULE 管理 DNS

Satellite 可使用您的 Capsule 管理 DNS 记录。DNS 管理包含从现有 DNS 区域更新和删除 DNS 记录。Capsule 具有多个 DNS 提供程序，可用于将 Satellite 与现有 DNS 基础架构集成或部署新的 DNS 提供程序。

启用 DNS 后，您的 Capsule 可以使用 dns_nsupdate 供应商操作任何符合 RFC 2136 的 DNS 服务器。其他提供商提供更多直接集成，如 Infoblox 的 dns_infoblox。

可用的 DNS 提供商

- dns_infoblox - 如需更多信息，请参阅 置备主机 中的 使用 Infoblox 作为 DHCP 和 DNS 提供商。
- dns_nsupdate - 使用 nsupdate 进行动态 DNS 更新。如需更多信息，请参阅 置备主机 中的 使用 Infoblox 作为 DHCP 和 DNS 提供商。
- dns_nsupdate_gss - 使用 GSS-TSIG 进行动态 DNS 更新。更多信息请参阅 第 4.4.1 节 “使用 GSS-TSIG 身份验证配置动态 DNS 更新”。

附录 A. CAPSULE 服务器扩展注意事项

Satellite 服务器支持的最大 Capsule 服务器数量没有固定限制。测试的限制为使用 Red Hat Enterprise Linux 7 的 Satellite 服务器上有 2 个 vCPU 的 17 个 Capsule 服务器。但是，可扩展性是高度变量，特别是在管理 Puppet 客户端时。

管理 Puppet 客户端时的 Capsule 服务器可扩展性取决于 CPU 数量、运行间隔分布和 Puppet 管理的资源数量。Capsule 服务器的限制为 100 个并发 Puppet 代理，在任何时间点上运行。运行超过 100 个并发 Puppet 代理会导致 503 HTTP 错误。

例如，假设 Puppet 代理运行不少于 100 个并发 Puppet 代理在 run-interval 期间在任何单一点运行，一个具有 4 个 CPU 的 Capsule 服务器具有最多 1250047-39）1600 Puppet 客户端，每个 Puppet 客户端分配有 10 个 Puppet 类。根据所需的 Puppet 客户端数量，Satellite 安装可以扩展 Capsule 服务器的数量来支持它们。

如果要在管理 Puppet 客户端时扩展 Capsule 服务器，则进行以下假设：

- 没有外部 Puppet 客户端直接报告 Satellite 集成胶囊。
- 所有其他 Puppet 客户端直接报告外部 Capsule。
- 所有 Puppet 代理都有平均分布式 run-interval。

注意

从甚至分发的版本会增加过度加载 Satellite 服务器的风险。应用 100 个并发请求的限值。

下表描述了使用推荐的 4 个 CPU 的可扩展性限制。

表 A.1. 使用 4 个 CPU 的 Puppet 可扩展性

每个主机的 Puppet 受管资源	运行时分发
1	3000 – 2500

每个主机的 Puppet 受管资源	运行时分发
10	2400 – 2000
20	1700 – 1400

下表描述了使用最少 2 个 CPU 的可扩展性限制。

表 A.2. 使用 2 个 CPU 的 Puppet 可扩展性

每个主机的 Puppet 受管资源	运行时分发
1	1700 – 1450
10	1500 – 1250
20	850 – 700