SUSE Manager 4.3

管理指南

2024年11月18日

SUSE

目录

管理指南概述 1

1. 操作 2

1.1. 重复性操作 2

1.2. 操作链 3

1.3. 远程命令 4

2. Ansible 集成 6

2.1. 功能概述 6

2.2. 要求和基本配置 6

2.3. 库存检查 6

2.4. 剧本发现 7

2.5. 剧本执行 7

2.6. 设置 Ansible 控制节点 7

2.6.1. 安装 SCAP 安全指南软件包 7

2.6.2. 创建 Ansible 库存文件 8

2.6.3. 与 Ansible 节点建立通信 9

2.7. 合规性即代码 9

2.7.1. 使用 Ansible 剧本运行修复 9

3. 身份验证方法 11

3.1. 使用单点登录 (SSO) 进行身份验证 11

3.1.1. 先决条件 11

3.1.2. 启用 SSO 12

3.1.3. 示例 SSO 实现 13

3.2. 使用 PAM 进行身份验证 16

4. 备份和还原 18

4.1. 备份 SUSE Manager 18

4.2. 使用 smdba 管理数据库 19

4.3. 使用 smdba 备份数据库 20

4.3.1. 执行手动数据库备份 20

4.3.2. 安排自动备份 21

4.4. 从备份中还原 22

4.5. 存档日志设置 22

4.6. 检索有关占用的数据库空间的概览 23

4.7. 移动数据库 23

4.8. 根分区崩溃后进行恢复 24

4.9. 数据库连接信息 25

5. 内容暂存 26
5.1. 启用内容暂存 26
5.2. 配置内容暂存 26
6. 通道管理 28
6.1. 通道管理 28
6.2. 删除通道 28
6.3. 相关主题 29
6.4. 自定义通道 29
6.4.1. 创建自定义通道和储存库 29
6.4.2. 自定义通道同步 32
6.4.3. 将软件包和补丁添加到自定义通道 33
6.4.4. 管理自定义通道 34
7. 内容生命周期管理 35
7.1. 创建内容生命周期项目 35
7.2. 过滤器类型 36
7.2.1. 过滤器规则参数 37
7.3. 过滤器模板 37
7.3.1. 根据 SUSE 产品在线增补 37
7.3.2. 根据系统在线增补 38
7.3.3. 含默认值的 AppStream 模块 39
7.4. 构建内容生命周期项目 39
7.5. 升级环境 40
7.6. 将客户端指派到环境 40
7.7. 内容生命周期管理示例 40
7.7.1. 为每月增补周期创建项目 40
7.7.2. 更新现有的每月增补周期 43
7.7.3. 使用在线增补增强项目 43
7.7.4. 切换到在线增补的新内核版本 44
7.7.5. AppStream 过滤器 44
8. 断开连接的设置 47
8.1. 同步 RMT 47
8.2. 同步 SMT 48
8.3. 必需通道 49
8.4. 同步已断开连接的服务器 49
9. 管理磁盘空间 51
9.1. 受监视的目录 51
9.2. 阈值 51

9.3. 关闭服务 51
9.4. 禁用空间检查 52
10. 映像构建和管理 53
10.1. 映像构建概述 53
10.2. 容器映像 53
10.2.1. 要求 54
10.2.2. 创建构建主机 54
10.2.3. 为容器创建激活密钥 54
10.2.4. 创建映像存储区 55
10.2.5. 创建映像配置文件 56
10.2.6. 构建映像 59
10.2.7. 导入映像 60
10.2.8. 查错 60
10.3. 操作系统映像 61
10.3.1. 要求 61
10.3.2. 创建构建主机 61
10.3.3. 为操作系统映像创建激活密钥 63
10.3.4. 创建映像存储区 64
10.3.5. 创建映像配置文件 64
10.3.6. 构建映像 67
10.3.7. 查错 68
10.3.8. 限制 69
10.4. 构建的映像列表 69
11. 基础结构维护任务 71
11.1. 服务器 71
11.1.1. 客户端工具 72
11.2. 服务器间同步从属服务器 72
11.3. 监视服务器 72
11.4. 代理 72
12. 服务器间同步 73
12.1. 服务器间同步 - 版本 1 73
12.2. 服务器间同步 - 版本 2 74
12.2.1. 安装 ISS 软件包 74
12.2.2. 内容同步 74
12.2.3. 数据库连接配置 75
12.2.4. 已知限制 75
13. SUSE Manager 的在线增补 76

13.1. 设置在线增补通道 76
13.1.1. 为在线增补使用 spacewalk-manage-channel-lifecycle 76
13.2. SLES 15 上的在线增补 77
13.3. SLES 12 上的在线增补 79
14. 维护时段 81
14.1. 维护日程安排类型 82
14.2. 受限制和非受限操作 83
15. 使用 mgr-sync 85
16. 使用 Prometheus 和 Grafana 进行监视 87
16.1. Prometheus 和 Grafana 87
16.1.1. Prometheus 87
16.1.2. Prometheus 导出器 87
16.1.3. Grafana 88
16.2. 设置监视服务器 88
16.2.1. 安装 Prometheus 88
16.2.2. 安装 Grafana 90
16.3. 配置 SUSE Manager 监视 92
16.3.1. 服务器自我监视 92
16.3.2. 监视受管系统 94
16.3.3. 更改 Grafana 口令 96
16.4. 网络边界 96
16.4.1. 反向代理设置 96
16.5. 安全 97
16.5.1. 生成 TLS 证书 97
17. 组织 98
17.1. 管理组织 98
17.1.1. 组织用户 98
17.1.2. 受信任组织 99
17.1.3. 配置组织 99
17.2. 管理状态 99
17.2.1. 管理配置通道 99
18. 补丁管理 100
18.1. 已收回补丁 100
18.1.1. 通道克隆 100
18.1.2. 补丁共享 101
19. 生成报告 102
19.1. 使用 spacewalk-report 102

19.2. spacewalk-report 和报告数据库 102
19.3. 可用报告列表 103
20. 安全 107
20.1. 设置用于客户端到主控端验证的指纹 107
20.2. 为储存库元数据签名 107
20.3. 镜像源软件包 109
20.4. 使用 OpenSCAP 确保系统安全 109
20.4.1. 关于 SCAP 109
20.4.2. 为客户端的 SCAP 扫描做好准备 110
20.4.3. OpenSCAP 内容文件 111
20.4.4. 查找 OpenSCAP 配置文件 111
20.4.5. 执行审计扫描 112
20.4.6. 扫描结果 113
20.4.7. 修复 113
20.5. 审计 117
20.5.1. CVE 审计 118
20.5.2. CVE 状态 118
21. SSL 证书 120
21.1. 自我签名 SSL 证书 120
21.1.1. 重新创建现有的服务器证书 121
21.1.2. 创建新的 CA 证书和服务器证书 121
21.2. 导入 SSL 证书 122
21.2.1. 为新安装导入证书 122
21.2.2. 为新的 Proxy 安装导入证书 123
21.2.3. 替换证书 123
21.3. HTTP 严格传输安全性 124
22. 订阅匹配 126
22.1. 将客户端关联到订阅 126
23. 任务日程安排 128
23.1. 预定义的任务组 129
24. 微调更改日志 132
25. 用户 133
25.1. 停用和删除帐户 133
25.2. 管理员角色 133
25.3. 用户权限和系统 134
25.4. 用户和通道权限 134
25.5. 用户默认语言 134

25.5.1. 用户默认界面主题 135
26. 在 SUSE Manager 中使用 PTF 136
26.1. 了解 PTF 软件包 136
26.2. 安装 PTF 软件包 136
26.3. 安装 PTF 后 137
26.4. 去除软件包的已修补版本 137
26.5. 在客户端上去除软件包的已修补版本 138
27. 查错 139
27.1. 在公有云 (BYOS) 中设置使用不同数据磁盘的 SUSE Manager 139
27.2. 自动安装查错 141
27.3. 裸机系统查错 142
27.4. 对生命周期已结束产品的引导储存库进行查错 142
27.5. 对克隆的 Salt 客户端进行查错 143
27.6. 对损坏的储存库进行查错 143
27.7. 对包含有冲突软件包的自定义通道进行查错 143
27.8. 对禁用 FQDNS grain 时出现的问题进行查错 144
27.9. 磁盘空间查错 145
27.10. 防火墙查错 145
27.11. 对通过 WAN 连接在 SUSE Manager Server 与 Proxy
之间同步时间过长的问题进行查错 146
27.12. 非活动客户端查错 148
27.13. 服务器间同步查错 148
27.14. 本地颁发者证书查错 149
27.15. 登录超时查错 149
27.16. 邮件配置查错 150
27.17. 对使用 noexec 挂载 /tmp 时出现的问题进行查错 150
27.18. 对使用 noexec 挂载 /var/tmp 时出现的问题进行查错 150
27.19. 对“磁盘空间不足”错误进行查错 151
27.20. 通知查错 151
27.21. 对启用 OES 储存库时出现的问题进行查错 151
27.22. OSAD 和 jabberd 查错 152
27.23. 对软件包不一致问题进行查错 152
27.24. 对通过代理获取储存库信息时出现的问题进行查错 153
27.25. 对将 Grain 传递给启动事件时出现的问题进行查错 153
27.26. PAYG 查错 154
27.27. 配置代理后端的 Pay-as-you-go 154
27.28. 代理连接和 FQDN 查错 154
27.29. 对注册克隆的客户端时出现的问题进行查错 154

27.30. 对在 Web UI 中注册失败且未显示任何错误的问题进行查错 157
27.31. 对在删除传统客户端后将其注册为 Salt 受控端时出现的问题进行查错 157
27.32. 对注册传统 Red Hat 客户端时出现的问题进行查错 157
27.33. 对 Red Hat CDN 通道和多个证书进行查错 157
27.34. SUSE Manager Server 重命名查错 158
27.35. 对重新尝试设置目标系统时出现的问题进行查错 159
27.36. RPC 超时查错 160
27.37. 对 Salt 客户端显示为关闭状态的问题和 DNS 设置进行查错 160
27.38. Saltboot 公式查错 161
27.39. 对纲要升级失败的问题进行查错 161
27.40. 同步查错 162
27.41. Taskomatic 查错 163
27.42. 对 Web UI 无法加载的问题进行查错 164
28. GNU Free Documentation License 165

管理指南概述

更新日期：2024-11-18

本指南提供有关在 SUSE Manager Server 上执行管理任务的指导。

Chapter 1. 操作

您可以通过多种不同的方式管理对客户端执行的操作。

对于 Salt 客户端，您可以安排自动重复性操作，以按照指定的日程安排将 Highstate 或任意一组自定义状态应用于客户端。您可以将重复性操作应用于单个客户端、系统组中的所有客户端或整个组织。

在 Salt 和传统客户端上，都可以通过创建操作链来设置要按特定顺序执行的操作。可以提前创建和编辑操作链，并将其安排为在适当的时间运行。

您还可以在一个或多个 Salt 客户端上执行远程命令。使用远程命令可以向单个 Salt 客户端或者与搜索词匹配的所有客户端发出命令。

1.1. 重复性操作

可以对单个 Salt 客户端、系统组、组织中的所有客户端应用重复性操作。

SUSE Manager 目前支持将以下操作类型作为重复性操作：

- `Highstate`：执行 Highstate。
- 自定义状态：执行一组自定义状态。自定义状态可以是 SUSE Manager 提供的内部状态，也可以是用户创建的配置通道。

有关配置通道的详细信息，请参见 **Client-configuration › Configuration-management**。

过程：创建新的重复性操作

1. 要将重复性操作应用于单个客户端，请导航到系统，单击要为其配置日程安排的客户端，然后导航到重复性操作选项卡。
2. 要将重复性操作应用于系统组，请导航到**系统 › 系统组**，选择要为其配置日程安排的组，然后导航到重复性操作选项卡。
3. 单击 **[创建]**。
4. 从操作类型下拉列表中选择操作类型。
5. 键入新日程安排的名称。
6. 选择重复性操作的频率：
   - 每小时：键入每小时内过去的分钟数。 例如，如果指定 `15`，则在每小时过去 15 分钟后运行操作。
   - 每日：选择每日的时间。 例如，如果指定 `01:00`，则在 SUSE Manager Server 所在时区的每日 01:00 运行操作。
   - 每周：选择星期日期和该日期中的时间，以便在每周的指定时间执行操作。
   - 每月：选择月份日期和该日期中的时间，以便在每月的指定时间执行操作。
   - 自定义 `Quartz` 格式：要查看更详细的选项，请输入自定义 Quartz 字符串。 例如，要在每个月的每个星期六 02:15 运行重复性操作，请输入：

```
0 15 2 ? * 7
```

7. 可选：将测试模式开关切换为打开，以在测试模式下运行日程安排。
8. 对于自定义状态类型的操作，请从可用状态列表中选择状态，然后单击 **[保存更改]**。此操作只会保存当前选择的状态，而不会保存日程安排。
9. 在下一个窗格中，拖放所选状态使其按执行顺序排列，然后单击 **[确认]**。
10. 最后，单击 **[创建日程安排]** 保存设置，并查看现有日程安排的完整列表。

组织管理员可为组织中的所有客户端设置和编辑重复性操作。导航到**首页 › 我的组织 › 重复性操作**，即可看到适用于整个组织的所有重复性操作。

SUSE Manager 管理员可为所有组织中的所有客户端设置和编辑重复性操作。导航到**管理 › 组织**，选择要管理的组织，然后导航到**状态 › 重复性操作**选项卡。

> 重复性操作只可用于 Salt 客户端。将忽略组或组织中的传统客户端。

1.2. 操作链

如果您需要对客户端执行多个有序操作，可以创建一个操作链以确保遵循该顺序。

默认情况下，大多数客户端会在发出命令后立即执行操作。在某些情况下，操作需要很长时间，这可能意味着之后发出的操作会失败。例如，如果您指示客户端重引导，然后发出第二个命令，则第二个操作可能会失败，因为重引导仍在进行。为确保操作按正确的顺序进行，请使用操作链。

> 对于事务更新系统，操作链会在单个快照内执行，直到进行重引导操作。这可能会产生某些限制。
>
> 有关详细信息，请参见 **Client-configuration › Clients-slemicro**。

可以在传统客户端和 Salt 客户端上使用操作链。操作链可以包含任意数量、采用任意顺序的以下操作：

- **系统细节 › 远程命令**
- **系统细节 › 安排系统重引导**
- **系统细节 › 状态 › Highstate**
- **系统细节 › 软件 › 软件包 › 列出/去除**
- **系统细节 › 软件 › 软件包 › 安装**
- **系统细节 › 软件 › 软件包 › 升级**
- **系统细节 › 软件 › 补丁**
- **系统细节 › 软件 › 软件通道**
- **系统细节 › 配置**

- **映像 › 构建**

过程：创建新操作链

1. 在 SUSE Manager Web UI 中，导航到您要在操作链中执行的第一个操作。例如，导航到客户端的系统细节，然后单击 **[安排系统重引导]**。
2. 选中添加到字段，然后选择要将操作添加到的操作链：
   - 如果这是您的第一个操作链，请选择新建操作链。
   - 如果该操作链已存在，请从列表中选择它。
   - 如果您已有操作链，但想要创建一个新操作链，请键入新操作链的名称以创建该操作链。
3. 确认操作。 该操作不会立即执行，而是创建新的操作链，并在屏幕顶部显示一个确认此行为的蓝色条。
4. 继续将操作添加到操作链，方法是选中添加到字段并选择要将操作添加到的操作链的名称。
5. 添加完操作后，导航到**日程安排 › 操作链**并从列表中选择操作链。
6. 通过将操作拖放到正确的位置来重新排列操作顺序。 单击蓝色加号查看要对其执行操作的客户端。单击 **[保存]** 以保存更改。
7. 安排操作链的运行时间，然后单击 **[保存并安排]**。 如果您在不单击 **[保存]** 或 **[保存并安排]** 的情况下离开页面，将丢弃所有未保存的更改。

> 如果操作链中的某个操作失败，操作链将会停止，且不再执行其他操作。

可以通过导航到**日程安排 › 待执行的操作**来查看操作链中已安排的操作。

1.3. 远程命令

可以将客户端配置为远程运行命令。这样，在无法直接访问客户端的情况下，也可以向客户端发出脚本或单个命令。

此功能在 Salt 客户端上已自动启用，您无需执行任何其他配置。对于传统客户端，如果您已使用引导脚本注册客户端并已启用远程命令，则会启用该功能。您也可以使用以下过程手动启用该功能。

在开始之前，请确保您的客户端已订阅适用于其中所安装操作系统的工具子通道。有关订阅软件通道的详细信息，请参见 **Client-configuration › Channels**。

> 对于事务更新系统，需考虑到远程命令会在单个快照内运行。这可能会产生某些限制。
>
> 有关详细信息，请参见 **Client-configuration › Clients-slemicro**。

过程：将传统客户端配置为接受远程命令

1. 在客户端上的命令提示符下，使用软件包管理器安装 `rhncfg`、`rhncfg-client` 和 `rhncfg-actions` 软件包（如果尚未安装）。 例如：

```
zypper in rhncfg rhncfg-client rhncfg-actions
```

2. 在客户端上的命令提示符下，以 root 身份在本地配置目录中创建一个路径：

```
mkdir -p /etc/sysconfig/rhn/allowed-actions/script
```

3. 在新目录中创建名为 `run` 的空文件。 此文件授予 SUSE Manager Server 运行远程命令的权限：

```
touch /etc/sysconfig/rhn/allowed-actions/script/run
```

Salt 客户端是从其 `/tmp` 目录中运行远程命令。为确保远程命令准确执行，请勿使用 `noexec` 选项挂载 `/tmp`。有关详细信息，请参见 **Administration › Troubleshooting**。

从远程命令页面运行的所有命令将在客户端上以 root 身份执行。可以使用通配符在任意数量的系统上运行命令。请务必在仔细检查后再发出命令。

过程：在传统客户端上运行远程命令

1. 在 SUSE Manager Web UI 中，导航到系统，单击要在其上运行远程命令的客户端，然后导航到**细节 › 远程命令**选项卡。
2. 在作为用户运行字段中，键入要在客户端上运行命令的用户的用户 ID (UID)。 或者，可以在作为组运行字段中使用组 ID (GID) 指定一个组来运行命令。
3. 可选：在超时字段中，键入命令的超时期限，以秒为单位。 如果命令在此期限内未能执行，则它不会继续运行。
4. 在命令标签字段中，键入命令的名称。
5. 在脚本字段中，键入要执行的命令或脚本。
6. 选择执行命令的日期和时间，或将远程命令添加到操作链。
7. 单击 **[日程安排]** 以安排远程命令。

有关操作链的详细信息，请参见 **Reference › Schedule**。

过程：在 Salt 客户端上运行远程命令

1. 导航到 **Salt › 远程命令**。
2. 在第一个字段中的 `@` 符号之前，键入您要发出的命令。
3. 在第二个字段中的 `@` 符号之后，键入您要在其上发出命令的客户端。 可以键入单个客户端的受控端 `ID`，也可以使用通配符指定一系列客户端作为目标。
4. 单击 **[查找目标]** 查看指定为目标的客户端，并确认使用了正确的细节。
5. 单击 **[运行命令]** 向目标客户端发出命令。

Chapter 2. Ansible 集成

目前，支持的 Ansible 版本为 SUSE Linux Enterprise 15 客户端工具通道中随附的 2.9 (LTS)。Ansible 控制节点支持的操作系统版本为 SUSE Linux Enterprise Server 15 SP3 或更高版本。Ansible 软件也可用于 SUSE Manager Proxy 和 SUSE Manager for Retail Branch Server。对于运行非 SUSE Linux Enterprise 操作系统的控制节点，请使用发行套件随附的 Ansible 版本。

2.1. 功能概述

SUSE Manager 可让系统管理员操作其 Ansible 控制节点。支持的功能包括：

- 库存文件检查
- 发现剧本
- 执行剧本

更多信息：

- 库存是指受管 Ansible 节点的排序列表。有关如何整理库存的详细信息，请参见 https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.html。
- 剧本用于描述应如何管理库存。有关剧本的详细信息，请参见 https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_intro.html。

2.2. 要求和基本配置

要使用 Ansible 功能，您需要将已有的 Ansible 控制节点作为 Salt 客户端注册到 SUSE Manager Server。在 Web UI 中已注册系统的**系统细节 › 属性**页面上，必须启用附加系统类型列表中的 `Ansible 控制节点`系统类型。

启用 `Ansible 控制节点`系统类型后，通过在 Highstate 中添加 `ansible` 软件包即可确保在系统上安装该软件包，以及在**系统细节 › Ansible** 选项卡中激活 Ansible 功能。

接下来，在**系统细节 › Ansible › 控制节点**页面上配置 Ansible 剧本目录和库存文件的路径。对于库存路径，可以使用标准 Ansible 库存路径 `/etc/ansible/hosts`。对于剧本目录，可以使用存储剧本文件的控制节点上的任何目录。剧本目录中包含 `.yml` 文件或含有 `.yml` 文件的子目录。

有关如何安装和设置 Ansible 控制节点的信息，请参见 **Administration › Ansible-setup-control-node**。

2.3. 库存检查

定义库存路径后，您可以使用 SUSE Manager 检查其中的内容。

过程：从 Web UI 中检查库存

1. 在 SUSE Manager Web UI 中，导航到**系统细节 › Ansible › 库存**
2. 单击某个库存路径，在控制节点上实时执行库存检查。

2.4. 剧本发现

定义剧本目录后，可以在**系统细节 › Ansible › 剧本**页面上发现剧本。

与库存检查一样，剧本发现操作也是在控制节点上实时运行。

2.5. 剧本执行

可以在**系统细节 › Ansible › 剧本**页面中安排剧本执行。选择要执行的剧本后，可以从安排剧本执行对话框的库存路径下拉菜单中选择要执行的库存文件。如果您未选择任何内容，将使用控制节点中配置的默认库存。下拉菜单中填充了您在库存路径中定义的库存，以及在剧本目录中本地发现的库存。这些库存在剧本细节中显示为自定义库存项。您还可以输入任意库存路径。

然后，您可以选择剧本执行时间或选择操作链。最终，SUSE Manager 会在控制节点上将剧本作为操作来执行。可以在操作细节页面上查看操作结果。

2.6. 设置 Ansible 控制节点

要设置 Ansible 控制节点，请在 SUSE Manager Web UI 中执行以下步骤。

过程：设置 Ansible 控制节点

1. 在 SUSE Manager Web UI 中，导航到**管理 › 安装向导 › 产品**，校验是否已选择并同步 `SUSE Linux Enterprise Server 15 SP5 x86_64` 和 `SUSE Manager Client Tools for SLE 15 x86_64`。
2. 部署一个 SUSE Linux Enterprise Server 15 SP5 客户端。
3. 在 SUSE Manager Web UI 中，导航到客户端的**系统 › 概览**页面。选择**软件 › 软件通道**，并为客户端订阅通道 `SUSE Linux Enterprise Server 15 SP5 x86_64` 和 `SUSE Manager Client Tools for SLE 15 x86_64`。

   SUSE Manager 客户端工具包含 `ansible` 软件包。

4. 选择客户端的**细节 › 属性**。在附加系统类型列表中启用 `Ansible 控制节点`，然后单击 **[更新属性]**。
5. 导航到客户端概览页面，选择**状态 › Highstate**，然后单击 **[应用 Highstate]**。
6. 选择**事件**选项卡并校验 Highstate 的状态。

2.6.1. 安装 SCAP 安全指南软件包

要执行修复，您需要在 Ansible 控制节点上安装 SCAP 安全指南软件包。

过程：安装 SCAP 安全指南软件包

1. 在**系统 › 概览**中选择客户端。然后单击**软件 › 软件包 › 安装**。
2. 搜索 `scap-security-guide` 并安装适合您系统的软件包。有关软件包分发要求，请参见下表：

表格 1. SCAP 安全指南软件包要求

软件包名称	支持的系统
scap-security-guide	openSUSE、SLES12、SLES15
scap-security-guide-redhat	CentOS 7、CentOS 8、Fedora、Oracle Linux 7、Oracle Linux 8、RHEL7、RHEL8、RHEL9、Red Hat OpenStack Platform 10、Red Hat OpenStack Platform 13、Red Hat Virtualization 4、Scientific Linux
scap-security-guide-debian	Debian 9、Debian 10
scap-security-guide-ubuntu	Ubuntu 16.04、Ubuntu 18.04、Ubuntu 20.04

2.6.2. 创建 Ansible 库存文件

Ansible 集成工具会将剧本部署为库存文件。请为表 1 中列出的每个操作系统创建一个库存文件。

过程：创建 Ansible 库存文件

1. 创建主机并将其添加到由 Ansible 管理的库存文件。Ansible 库存的默认路径为 `/etc/ansible/hosts`。

列表 1. 库存示例

```
client240.mgr.example.org
client241.mgr.example.org
client242.mgr.example.org
client243.mgr.example.org ansible_ssh_private_key_file=/etc/ansible/some_ssh_key

[mygroup1]
client241.mgr.example.org
client242.mgr.example.org

[mygroup2]
client243.mgr.example.org

[all:vars]
ansible_ssh_private_key_file=/etc/ansible/my_ansible_private_key
```

2. 在 SUSE Manager Web UI 中的 `Ansible` 选项卡内，导航到 **Ansible › 控制节点**，将库存文件添加到该控制节点中。
3. 在剧本目录部分下，将 `/usr/share/scap-security-guide/ansible` 添加到添加剧本目录字段中，然后单击 **[保存]**。
4. 在库存文件下，将您的库存文件位置添加到添加库存文件字段，然后单击 **[保存]**。

列表 2. 示例

```
/etc/ansible/sles15
/etc/ansible/sles12
/etc/ansible/centos7
```

有关更多剧本示例，请参见 https://github.com/ansible/ansible-examples。

2.6.3. 与 Ansible 节点建立通信

过程：与 Ansible 节点建立通信

1. 创建您要在库存中使用的 SSH 密钥。

```
ssh-keygen -f /etc/ansible/my_ansible_private_key
```

2. 将生成的 SSH 密钥复制到 Ansible 受管客户端。示例：

```
ssh-copy-id -i /etc/ansible/my_ansible_private_key root@client240.mgr.example.org
```

3. 如下所示在 `/etc/ansible/ansible.cfg` 中声明私用密钥：

```
private_key_file = /etc/ansible/my_ansible_private_key
```

   请将 `my_ansible_private_key` 替换为包含私用密钥的文件的文件名。

4. 通过从控制节点执行以下命令来测试 Ansible 是否正常运行：

```
ansible all -m ping
ansible mygroup1 -m ping
ansible client240.mgr.example.org -m ping
```

现在您可以运行修复。

有关详细信息，请参见 **Administration › Ansible-compliance-as-code**。

2.7. 合规性即代码

本文档提供了有关使用 Ansible 剧本运行合规性即代码修复的深入信息。

有关使用 bash 脚本运行合规性即代码修复的详细信息，请参见修复。

2.7.1. 使用 Ansible 剧本运行修复

需要一个 Ansible 控制节点。有关详细信息，请参见 **Administration › Ansible-setup-control-node**。

以下过程将指导您使用 Ansible 剧本运行修复。

过程：使用 Ansible 剧本运行修复

1. 在控制节点系统菜单中选择 **Ansible › 剧本**。展开文件夹选项卡，然后选择一个剧本。
2. 单击该剧本。
3. 要运行该剧本，请选择客户端的操作系统**库存路径**，例如：

```
/etc/ansible/sles15
```

4. 单击 **[日程安排]**。
5. 在事件选项卡下检查已安排事件的状态。

Chapter 3. 身份验证方法

SUSE Manager 支持多种不同的身份验证方法。本章介绍可插入身份验证模块 (PAM) 和单点登录 (SSO)。

3.1. 使用单点登录 (SSO) 进行身份验证

SUSE Manager 通过实现安全声明标记语言 (SAML) 2 协议来支持单点登录 (SSO)。

单点登录是一种身份验证过程，它允许用户使用一组身份凭证访问多个应用程序。SAML 是一套基于 XML 的标准，用于交换身份验证和授权数据。SAML 身份服务提供者 (IdP) 向服务提供者 (SP) 提供身份验证和授权服务，例如 SUSE Manager。SUSE Manager 公开三个端点，必须启用它们才能进行单点登录。

SUSE Manager 中的 SSO 支持：

- 使用 SSO 登录。
- 使用服务提供者发起的单点注销 (SLO) 和身份服务提供者单点注销服务 (SLS) 注销。
- 声明和 nameId 加密。
- 声明签名。
- 使用 AuthNRequest、LogoutRequest 和 LogoutResponses 进行消息签名。
- 启用声明使用者服务端点。
- 启用单点注销服务端点。
- 发布 SP 元数据（可签名）。

SUSE Manager 中的 SSO 不支持：

- 身份服务提供者 (IdP) 的产品选择和实现。
- 对其他产品的 SAML 支持（请查看相关的产品文档）。

有关 SSO 的示例实现，请参见 **Administration › Auth-methods-sso-example**。

> 如果您从默认身份验证方法更改为单点登录，则新的 SSO 身份凭证仅适用于 Web UI。`mgr-sync` 或 `spacecmd` 等客户端工具仍然只能使用默认身份验证方法。

3.1.1. 先决条件

在开始之前，需要事先使用这些参数配置一个外部身份服务提供者。请查看 IdP 文档获取说明。

> 您的 IdP 必须有一个 SAML:Attribute，其中包含 IdP 用户域的用户名，称为 `uid`。在激活单点登录之前，必须在 SUSE Manager 用户库中创建在 SAML:Attribute 中传递的 `uid` 属性。

需要以下端点：

- 声明使用者服务 (ACS)：接受 SAML 消息以建立与服务提供者的会话的端点。 SUSE Manager 中 ACS 的端点是：https://server.example.com/rhn/manager/sso/acs
- 单点注销服务 (SLS)：从 IdP 发起注销请求的端点。 SUSE Manager 中 SLS 的端点是：https://server.example.com/rhn/manager/sso/sls
- 元数据：用于检索 SAML 的 SUSE Manager 元数据的端点。 SUSE Manager 中元数据的端点是：https://server.example.com/rhn/manager/sso/metadata

使用用户 `orgadmin` 成功通过 IdP 完成身份验证后，您将以 `orgadmin` 用户身份登录到 SUSE Manager，前提是 SUSE Manager 中存在 `orgadmin` 用户。

3.1.2. 启用 SSO

SSO 与其他类型的身份验证是互斥的：请要么启用，要么禁用 SSO。默认已禁用 SSO。

过程：启用 SSO

1. 如果您的用户在 SUSE Manager 中尚不存在，请先创建他们。
2. 编辑 `/etc/rhn/rhn.conf`，在文件末尾添加下面一行：

```
java.sso = true
```

3. 在 `/usr/share/rhn/config-defaults/rhn_java_sso.conf` 中找到您要自定义的参数。 将要自定义的参数插入 `/etc/rhn/rhn.conf`，并在这些参数的前面加上 `java.sso.` 作为前缀。例如，在 `/usr/share/rhn/config-defaults/rhn_java_sso.conf` 中找到：

```
onelogin.saml2.sp.assertion_consumer_service.url = https://YOUR-PRODUCT-HOSTNAME-OR-IP/rhn/manager/sso/acs
```

要自定义此参数，请在 `/etc/rhn/rhn.conf` 中创建相应的选项并在选项名称前面加上`java.sso.` 作为前缀：

```
java.sso.onelogin.saml2.sp.assertion_consumer_service.url = https://YOUR-PRODUCT-HOSTNAME-OR-IP/rhn/manager/sso/acs
```

要查找您需要更改的所有参数实例，请在文件中搜索占位符 `YOUR-PRODUCT` 和 `YOUR-IDP-ENTITY`。每个参数都附带了其作用的简要说明。

4. 重启动 spacewalk 服务以应用更改：

```
spacewalk-service restart
```

访问 SUSE Manager URL 时，您将重定向到 SSO 的 IdP，需要在其中完成身份验证。身份验证成功后，您将重定向到 SUSE Manager Web UI，并以经过身份验证的用户身份登录。如果您在使用 SSO 登录时遇到问题，请查看 SUSE Manager 日志了解详细信息。

3.1.3. 示例 SSO 实现

此示例通过使用 SUSE Manager 公开三个端点并使用 Keycloak 21.0.1 或更高版本作为身份服务提供者 (IdP) 来实现 SSO。

首先安装 Keycloak IdP，然后设置 SUSE Manager 服务器。之后可以将端点添加为 Keycloak 客户端并创建用户。

> 此示例仅用于说明目的。SUSE 不建议也不支持第三方身份服务提供者，并且与 Keycloak 不存在从属关系。有关 Keycloak 支持信息，请参见 https://www.keycloak.org/。

可以直接在您的计算机上安装 Keycloak，或者在容器中运行 Keycloak。此示例在 Podman 容器中运行 Keycloak。有关安装 Keycloak 的详细信息，请参见 https://www.keycloak.org/guides#getting-started 上的 Keycloak 文档。

过程：设置身份服务提供者

1. 根据 Keycloak 文档所述在 Podman 容器中安装 Keycloak。
2. 使用 `-td` 参数运行容器，以确保进程保持运行：

```
podman run -td --name keycloak -p 8080:8080 -e KEYCLOAK_USER=admin -e
KEYCLOAK_PASSWORD=admin quay.io/keycloak/keycloak:21.0.1
```

3. 以 `admin` 用户身份登录到 Keycloak Web UI，然后使用以下细节创建身份验证领域：
   - 在名称字段中输入领域的名称。 例如 `SUMA`。
   - 在端点字段中，单击 `SAML 2.0 身份提供者元数据`链接。 如此您将转到一个页面，其中会显示要复制到 SUSE Manager 配置文件中的端点和证书。

安装 Keycloak 并创建领域后，便可以准备 SUSE Manager 服务器。

过程：设置 SUSE Manager Server

1. 在 SUSE Manager Server 上打开 `/etc/rhn/rhn.conf` 配置文件，然后编辑这些参数。 将 `<FQDN_SUMA>` 替换为您的 SUSE Manager 安装的完全限定域名：

```
java.sso.onelogin.saml2.sp.entityid                =
https://<FQDN_SUMA>/rhn/manager/sso/metadata
java.sso.onelogin.saml2.sp.assertion_consumer_service.url =
https://<FQDN_SUMA>/rhn/manager/sso/acs
java.sso.onelogin.saml2.sp.single_logout_service.url     =
https://<FQDN_SUMA>/rhn/manager/sso/sls
```

2. 在配置文件中，将 `<FQDN_IDP>` 替换为您的 Keycloak 服务器的完全限定域名。 将 `<REALM>` 替换为您的身份验证领域，例如 `SUMA`：

```
java.sso.onelogin.saml2.idp.entityid              = http://<FQDN_IDP>:8080/realms/<REALM>
java.sso.onelogin.saml2.idp.single_sign_on_service.url =
http://<FQDN_IDP>:8080/realms/<REALM>/protocol/saml
java.sso.onelogin.saml2.idp.single_logout_service.url  =
http://<FQDN_IDP>:8080/realms/<REALM>/protocol/saml
```

3. 在 IdP 元数据中，找到公共 x509 证书。 证书使用如下格式：http://<FQDN_IDP>:8080/realms/<REALM>/protocol/saml/descriptor。在配置文件中指定 IdP 的公共 x509 证书：

```
java.sso.onelogin.saml2.idp.x509cert = -----BEGIN CERTIFICATE----- <CERTIFICATE>  -----END
CERTIFICATE-----
```

下面是启用 SSO 后 SUSE Manager 上的 `rhn.conf` 的示例：

```
java.sso = true


# This is the configuration file for Single Sign-On (SSO) via SAMLv2 protocol
# To enable SSO, set java.sso = true in /etc/rhn/rhn.conf
#
# Mandatory changes: search this file for:
# - YOUR-PRODUCT
# - YOUR-IDP-ENTITY
#
# See product documentation and the comments inline in this file for more
# information about every parameter.
#
#
#
#
# If 'strict' is True, then the Java Toolkit will reject unsigned
# or unencrypted messages if it expects them signed or encrypted
# Also will reject the messages if not strictly follow the SAML
#
# WARNING: In production, this parameter setting parameter MUST be set as "true".
# Otherwise your environment is not secure and will be exposed to attacks.
# Enable debug mode (to print errors)
# Identifier of the SP entity (must be a URI)
java.sso.onelogin.saml2.sp.entityid =
https://sumaserver.example.org/rhn/manager/sso/metadata

# Specifies info about where and how the <AuthnResponse> message MUST be
# returned to the requester, in this case our SP.
# URL Location where the <Response> from the IdP will be returned
java.sso.onelogin.saml2.sp.assertion_consumer_service.url =
https://sumaserver.example.org/rhn/manager/sso/acs

# Specifies info about where and how the <Logout Response> message MUST be
# returned to the requester, in this case our SP.
java.sso.onelogin.saml2.sp.single_logout_service.url =
https://sumaserver.example.org/rhn/manager/sso/sls

# Identifier of the IdP entity (must be a URI)
java.sso.onelogin.saml2.idp.entityid = http://idp.example.org:8080/realms/SUMA

# SSO endpoint info of the IdP. (Authentication Request protocol)
# URL Target of the IdP where the SP will send the Authentication Request Message
java.sso.onelogin.saml2.idp.single_sign_on_service.url =
http://idp.example.org:8080/realms/SUMA/protocol/saml

# SLO endpoint info of the IdP.
# URL Location of the IdP where the SP will send the SLO Request
java.sso.onelogin.saml2.idp.single_logout_service.url =
```

```
http://idp.example.org:8080/realms/SUMA/protocol/saml

# Public x509 certificate of the IdP
java.sso.onelogin.saml2.idp.x509cert = -----BEGIN CERTIFICATE-----
MIIClzCCAX8CBgGC+tPbVjANBgkqhkiG9w0BAQsFADAPMQ0wCwYDVQQDDARTVU1BMB4XDTIyMD
kwMTIwNTEwNFoXDTMyMDkwMTIwNTI0NFowDzENMAsG
A1UEAwwEU1VNQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMNSWJAalB5mShT
kMBO5mrsOosyheEL8/A37WvuqDPwwEfm4x0cG7gmMHvONxYXZk+LRyzoQl2sBrNFrbMuwu5dna
h5ZSMxQyUu697S280m4vIiegGaFdbgH+g4FGBu
eSis1ssMzTcES+NUuI7pLkMLNmSQtncESnoL9q2SyeQSwYtr5dz1ydl6IzjwtaWeyQ9EGJNtJtLk3U4
+arLPCpHAwqFAnLO9NeYcRDNUKhNBs1v5mHP+L066PZu1/DkE0mSgy/+qXaS0CgZVKqz8qB+bv
HVuAq9W60g1CjqZKbwvPu72p/7+d8z
9DxXPlZ1uxdqn19q/kLEP2TYLtgQobSHECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAga+raLMJD
o/P/yN1Z6SGGocK227WFqovBiE/mLYlp5Ff0+0jS1US1plSppJ94xOr8j0m7HW0Wu5xCz6oOhzXTEt
nfIbeRyr1Rms3BWdxyXgQ9bWUeZMWZ
HfDkTbhgRRmjDEwSSfEXRKQNvw41CpnlB36I0++ejgGnjDvH7BbkCaoW55JF5j6DT/WYR0n7MkEl2
Ova9CH0e9X7Gny8iOAg26oziy06uy3P/lx9Z9RmHnvpvN/Q34SGEq9z/HlQVuP12UPj//iT21Jc17OO
ZFsZQXlGFTG6bXKmO42W8FdUDJU
ONoXZgjMb3eC7U691YyeowoqTY7mJKxNPprYY/lL0w== -----END CERTIFICATE-----

# Organization
java.sso.onelogin.saml2.organization.name = SUSE Manager admin
java.sso.onelogin.saml2.organization.displayname = SUSE Manager admin
java.sso.onelogin.saml2.organization.url = https://sumaserver.example.org
java.sso.onelogin.saml2.organization.lang =

# Contacts
java.sso.onelogin.saml2.contacts.technical.given_name = SUSE Manager admin
java.sso.onelogin.saml2.contacts.technical.email_address = suma@example.org
java.sso.onelogin.saml2.contacts.support.given_name = SUSE Manager admin
java.sso.onelogin.saml2.contacts.support.email_address = suma@example.org
```

您可以将 SUSE Manager 端点添加到 Keycloak 中。Keycloak 将端点称为客户端。

过程：将端点添加为客户端

1. 在 Keycloak Web UI 中，使用以下细节创建新客户端：
   - 在客户端类型字段中选择 `SAML`。
   - 在客户端 `ID` 字段中，输入服务器配置文件中以 `java.sso.onelogin.saml2.idp.entityid` 形式指定的端点。 例如 https://<FQDN_SUMA>/rhn/manager/sso/metadata。
2. 在设置选项卡中，使用以下细节对客户端进行精细调整：
   - 将对声明签名开关切换为开。
   - 在签名算法字段中选择 `RSA_SHA1`。
   - 在 `SAML` 签名密钥名称字段中，选择密钥 `ID`。
3. 在密钥选项卡中：
   - 将需要客户端签名切换为关。
4. 在高级选项卡上的精细 `SAML` 端点配置部分，使用以下细节添加两个端点：
   - 在声明使用者服务字段中，输入服务器配置文件中以 `java.sso.onelogin.saml2.sp.assertion_consumer_service.url` 形式指定的端点。 例如 https://<FQDN_SUMA>/rhn/manager/sso/acs。
   - 在注销服务字段中，输入服务器配置文件中以 `java.sso.onelogin.saml2.sp.single_logout_service.url` 形式指定的端点。 例如 https://<FQDN_SUMA>/rhn/manager/sso/sls。

将端点添加为客户端后，可以配置客户端范围，并在 Keycloak 和 SUSE Manager 之间映射用户。

过程：配置客户端范围和映射程序

1. 在 Keycloak Web UI 中，导航到**客户端 › 客户端范围**选项卡，然后将 `role_list` 指定为默认客户端范围。
2. 导航到**客户端范围 › 映射程序**选项卡，然后使用默认值添加用户属性 `UID` 的映射程序。 SUSE Manager 需要此 SAML 属性。
3. 导航到**客户端范围 › 映射程序**，然后单击 `role_list` 映射程序。将单角色属性设置为开。
4. 导航到**用户 › 管理员**部分并创建一个管理用户。 此用户不需要与 SUSE Manager 管理用户匹配。
5. 导航到**用户 › 角色映射**选项卡，使用与 SUSE Manager 管理用户的用户名匹配的值添加名为 `UID` 的属性。
6. 导航到**用户 › 身份凭证**选项卡，设置 SUSE Manager 管理用户所用的同一口令。
7. 保存更改。

完成配置后，可以测试安装是否按预期工作。重启动 SUSE Manager 服务器以应用您的更改，然后导航到 SUSE Manager Web UI。如果您的安装正常工作，则您会重定向到 Keycloak SSO 页面，可在其中成功完成身份验证。

3.2. 使用 PAM 进行身份验证

SUSE Manager 支持使用可插入身份验证模块 (PAM) 的基于网络的身份验证系统。PAM 是一个库套件，可用于将 SUSE Manager 与集中式身份验证机制集成，从而无需记住多个口令。SUSE Manager 支持 LDAP、Kerberos 和其他使用 PAM 的基于网络的身份验证系统。

在用户名中，除了字母数字字符外，还允许使用 `-`、`_`、`.` 和 `@`。

过程：启用 PAM

1. 在 `/etc/pam.d/susemanager` 中创建一个 PAM 服务文件。文件名必须采用小写，并且可以由 `tomcat` 用户读取。SUSE Manager 使用此文件来加载正确的 PAM 配置文件：

```
#%PAM-1.0
auth    include      common-auth
account  include      common-account
password include      common-password
session  include      common-session
```

列表 3. 在 SUSE Manager Server 上的命令提示符下，以 root 身份添加 `sss` PAM 模块：

```
pam-config -a --sss
```

此命令将模块添加到 `/etc/pam.d/common-auth` 配置文件。我们不建议直接编辑此文件。

2. 通过将下面一行内容添加到 `/etc/rhn/rhn.conf` 来强制使用服务文件：

```
pam_auth_service = susemanager
```

在此示例中，PAM 服务文件名为 `susemanager`。

3. 更改配置后重启动 SUSE Manager 服务。
4. 在 SUSE Manager Web UI 中，导航到**用户 › 创建用户**，并允许新用户或现有用户使用 PAM 进行身份验证。
5. 选中可插入身份验证模块（PAM）复选框。该复选框位于口令和口令确认字段下方。

> 在 SUSE Manager Web UI 中更改口令只会更改 SUSE Manager Server 上的本地口令。如果为该用户启用 PAM，则可能根本不会使用本地口令。例如，在上面的示例中，Kerberos 口令并未更改。使用网络服务的口令更改机制来更改这些用户的口令。

要配置系统范围的身份验证，可以使用 YaST。需要安装 `yast2-auth-client` 软件包。

有关配置 PAM 的详细信息，请参见《SUSE Linux Enterprise Server 安全指南》，其中提供了一个通用示例，该示例同样适用于其他基于网络的身份验证方法。其中还介绍了如何配置 Active Directory 服务。有关详细信息，请参见 https://documentation.suse.com/sles/15-SP4/html/SLES-all/part-auth.html。

Chapter 4. 备份和还原

定期备份您的 SUSE Manager 安装以防数据丢失。由于 SUSE Manager 依赖于某个数据库以及已安装的程序和配置，因此备份所有安装组件非常重要。本章包含有关需要备份的文件的信息，并介绍如何使用 `smdba` 工具来管理数据库备份。其中还包含有关在发生系统故障时如何从备份中还原的信息。

> 无论您使用哪种备份方法，可用空间必须是当前安装使用的空间量的至少三倍。空间不足可能导致备份失败，因此请经常检查可用空间。

4.1. 备份 SUSE Manager

备份 SUSE Manager 安装的最完整方法是备份相关文件和目录。这可以节省备份管理时间，并且在发生故障时可以更快地重新安装和重新同步。但是，这种方法需要大量磁盘空间，并且可能需要很长时间才能完成备份。

> 如果您只想备份所需的文件和目录，请使用以下列表。为使此过程更简单、更完整，我们建议备份整个 `/etc` 和 `/root` 目录，而不仅仅是此处指定的目录。某些文件仅在您实际使用相关 SUSE Manager 功能时才存在。

- `/etc/cobbler/`
- `/etc/dhcp.conf`
- `/etc/fstab` 和所需的任何 ISO 挂载点。

  如果您的 UUID 已更改，请确保已相应地更新 `fstab` 项。

- `/etc/rhn/`
- `/etc/salt`
- `/etc/sudoers`
- `/etc/sysconfig/rhn/`
- `/root/.gnupg/`
- `/root/.ssh`

  如果您使用 SSH 隧道或 SSH `push`，则此文件存在。此外，必须已保存 `id-susemanager` 键的副本。

- `/root/ssl-build/`
- `/srv/formula_metadata`
- `/srv/pillar`
- `/srv/salt`
- `/srv/susemanager`
- `/srv/tftpboot/`
- `/srv/www/cobbler`

- /srv/www/htdocs/pub/
- /srv/www/os-images
- /var/cache/rhn
- /var/cache/salt
- /var/lib/cobbler/
- /var/lib/cobbler/templates/（在 4.0 版之前为 /var/lib/rhn/kickstarts/）
- /var/lib/Kiwi
- /var/lib/rhn/
- /var/run/pgsql/
- /var/lib/salt/
- /var/run/salt/
- /var/spacewalk/
- 包含自定义数据（例如脚本、Kickstart 或 AutoYaST 配置文件）和自定义 RPM 的任何目录。

还需要备份您的数据库，此操作可以使用 smdba 工具来完成。

过程：从手动备份中还原

1. 重新安装 SUSE Manager Server。有关详细信息，请参见 **Installation-and-upgrade › Install-server-unified**。
2. 使用 yast2 susemanager_setup 安装 SUSE Manager Server。有关详细信息，请参见 **Installation-and-upgrade › Server-setup**。
3. 使用 SUSE Manager Web UI 或在命令提示符下使用 mgr-sync 工具重新同步您的 SUSE Manager 储存库。您可以选择重新注册产品，或跳过注册和 SSL 证书生成部分。
4. 重新安装 /root/ssl-build/rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm 软件包。
5. 安排在下次启动 rhn-search 服务时重新创建搜索索引。此命令仅生成调试消息，而不生成错误消息：

```
rhn-search cleanindex
```

6. 检查是否需要还原 /var/spacewalk/packages/。如果 /var/spacewalk/packages/ 不在您的备份中，则需要还原它。如果源储存库可用，则您可以通过完整通道同步来还原 /var/spacewalk/packages/：

```
mgr-sync refresh --refresh-channels
```

4.2. 使用 smdba 管理数据库

smdba 工具用于管理本地 PostgreSQL 数据库。您可以使用它来备份并还原数据库，以及管理备份。它还可用于检查数据库的状态、执行重启动等管理任务。

smdba 工具仅适用于本地 PostgreSQL 数据库，而不适用于远程访问的数据库或 Oracle 数据库。

> smdba 工具需要 sudo 访问权限，以便能够执行系统更改。在开始之前，请通过检查 /etc/sudoers 文件中的下面一行，来确保为 admin 用户启用了 sudo 访问权限：
>
> ```
> admin ALL=(postgres) /usr/bin/smdba
> ```

使用以下命令检查数据库的运行时状态：

```
smdba db-status
```

此命令返回 online 或 offline，例如：

```
Checking database core... online
```

可使用以下命令启动和停止数据库：

```
smdba db-start
```

和：

```
smdba db-stop
```

4.3. 使用 smdba 备份数据库

smdba 工具执行连续存档备份。这种备份方法将合并当前会话期间对数据库所做和每项更改的日志，以及一系列较传统的备份文件。发生崩溃时，首先会从磁盘上和最近备份文件中还原数据库状态，然后精确重放当前会话的日志，使数据库恢复到当前状态。smdba 连续存档备份是在数据库正在运行的情况下执行的，因此无需停机。

这种备份方法非常稳定，通常会创建一致的快照，但可能会占用大量存储空间。请确保至少提供当前数据库大小三倍的可用空间用于备份。可以通过导航到 /var/lib/pgsql/ 并运行 df -h 来检查当前数据库大小。

smdba 工具还可以管理存档，仅保留最近的备份和当前日志存档。日志文件的最大文件为 16 MB，因此，当文件达到此大小时会创建一个新日志文件。每次创建新备份时，会清除以前的备份以释放磁盘空间。我们建议您使用 cron 来安排 smdba 备份以确保您的存储得到有效管理，并随时准备好一个备份，以防发生故障。

4.3.1. 执行手动数据库备份

smdba 工具可直接从命令行运行。我们建议您在安装后立即运行手动数据库备份，或者在对配置进行任何重大更改后运行手动备份。

> 首次运行 smdba 或者更改了备份位置时，需要先重启动数据库，然后再执行存档。这会导致短暂的停机。定期数据库备份完全不需要停机。

过程：执行手动数据库备份

1. 为备份分配永久存储空间。此示例使用 `/var/spacewalk/` 中的目录。此目录将成为备份的永久目标，因此请确保您的服务器始终可以访问此目录。
2. 在您的备份位置为备份创建一个目录：

   以 root 身份运行以下命令：

   ```
   install -d -o postgres -g postgres -m 700 /var/spacewalk/db-backup
   ```

3. 确保您对备份位置拥有适当的权限：

   ```
   chown postgres:postgres /var/spacewalk/db-backup
   ```

4. 首次创建备份时，请运行 `smdba backup-hot` 命令并设置 `enable` 选项。这会在指定的目录中创建备份，并根据需要重启动数据库：

   ```
   smdba backup-hot --enable=on --backup-dir=/var/spacewalk/db-backup
   ```

   此命令将生成调试消息，成功完成时会返回以下输出：

   ```
   信息：已完成
   ```

5. 检查 `/var/spacewalk/db-backup` 目录中是否存在备份文件，确保备份成功。

4.3.2. 安排自动备份

无需关闭系统即可使用 `smdba` 执行数据库备份。但是，由于备份是一项大规模操作，因此在运行备份时，数据库性能可能会下降。我们建议您将定期数据库备份安排在低流量时段，以尽量减少中断。

> 请确保至少提供当前数据库大小三倍的可用空间用于备份。可以通过导航到 `/var/lib/pgsql/` 并运行 `df -h` 来检查当前数据库大小。

过程：安排自动备份

1. 为备份创建一个目录并设置适当的权限（以 root 身份）：

   ```
   install -d -m 700 -o postgres -g postgres /var/spacewalk/db-backup
   ```

2. 打开 `/etc/cron.d/db-backup-mgr`（如果该文件不存在，请创建），并在其中添加下面一行内容以创建 cron 作业：

   ```
   0 2 * * * root /usr/bin/smdba backup-hot --enable=on --backup-dir=/var/spacewalk/db
   -backup
   ```

3. 定期检查备份目录以确保备份按预期进行。

4.4. 从备份中还原

发生故障时，可以使用 `smdba` 工具从备份中还原。

过程：从备份中还原

1. 关闭数据库：

```
smdba db-stop
```

2. 启动还原过程并等待它完成：

```
smdba backup-restore start
```

3. 重启动数据库：

```
smdba db-start
```

4. 检查 RPM 和数据库之间是否有差异。

```
spacewalk-data-fsck
```

4.5. 存档日志设置

数据库管理工具 `smdba` 可以通过存档日志记录来执行热备份。在包含嵌入式数据库的 SUSE Manager 中，默认已启用存档日志记录。

PostgreSQL 维护有限数量的存档日志。在使用默认配置的情况下，大约可以存储 64 个大小为 16 MiB 的文件。

创建用户并同步通道：

- SLES12-SP2-Pool-x86_64
- SLES12-SP2-Updates-x86_64
- SLE-Manager-Tools12-Pool-x86_64-SP2
- SLE-Manager-Tools12-Updates-x86_64-SP2

PostgreSQL 会额外生成大约 1 GB 数据。因此，请务必考虑备份策略并定期创建备份。

存档日志存储在 `/var/lib/pgsql/data/pg_xlog/` (postgresql) 中。

4.6. 检索有关占用的数据库空间的概览

数据库管理员可以使用子命令 `space-overview` 来获取有关占用的表空间的报告，例如：

```
smdba space-overview
```

输出：

```
SUSE Manager Database Control. Version 1.5.2
Copyright (c) 2012 by SUSE Linux Products GmbH

表空间  | 大小 (Mb) | 可用 (Mb) | 使用率
------------+-----------+------------+------
postgres   | 7       | 49168     | 0.013
susemanager | 776     | 48399     | 1.602
```

`smdba` 命令适用于 PostgreSQL。如需更详细的报告，请使用 `space-tables` 子命令。它可以列出表及其大小，例如：

```
smdba space-tables
```

输出：

```
SUSE Manager Database Control. Version 1.5.2
Copyright (c) 2012 by SUSE Linux Products GmbH

表                          | 大小
-------------------------------------+-----------
public.all_primary_keys            | 0 字节
public.all_tab_columns             | 0 字节
public.allserverkeywordsincereboot   | 0 字节
public.dblink_pkey_results         | 0 字节
public.dual                        | 8192 字节
public.evr_t                       | 0 字节
public.log                         | 32 kB
...
```

4.7. 移动数据库

可以将数据库移到另一个位置。例如，在数据库存储空间不足的情况下。

过程：移动数据库

1. SUSE Manager 的默认存储位置是 `/var/lib/pgsql/`。如果您想要移动此位置，例如移到 `/storage/postgres/`，请执行以下操作。
2. 在命令提示符下，以 root 身份停止正在运行的数据库：

   ```
   rcpostgresql stop
   ```

   关闭正在运行的 spacewalk 服务：

```
spacewalk-service stop
```

3. 结合 `-a`、`--archive` 选项使用 `cp` 复制当前工作目录结构。 例如：

```
cp --archive /var/lib/pgsql/ /storage/postgres/
```

此命令将 `/var/lib/pgsql/` 的内容复制到 `/storage/postgres/pgsql/`。

> `/var/lib/pgsql` 目录的内容需保持不变，否则 SUSE Manager 数据库可能会出现异常。您还应该确保有足够的可用磁盘空间。

4. 挂载新的数据库目录：

```
mount /storage/postgres/pgsql
```

5. 切换到新目录并运行以下命令，确保所有权是 `postgres:postgres` 而不是 `root:root`：

```
cd /storage/postgres/pgsql/
ls -l
```

输出：

```
total 8
drwxr-x---  4 postgres postgres   47 Jun  2 14:35 ./
```

6. 通过编辑 `etc/fstab` 将新数据库挂载位置添加到服务器的 fstab。
7. 使用以下命令启动数据库：

```
rcpostgresql start
```

8. 启动 spacewalk 服务：

```
spacewalk-service start
```

4.8. 根分区崩溃后进行恢复

如果您的根分区已崩溃，您可以通过一些额外的步骤重启动 SUSE Manager Server。本节假设您已为数据库和通道使用不同的分区设置了服务器，这两个分区分别挂载在 `/var/lib/pgsql` 和 `/var/spacewalk/` 位置。

> 安装新系统后，大多数用户和组将获得不同的 ID。大多数备份系统会存储名称而不是 ID，并将还原具有正确所有权和权限的文件。但是，如果您挂载现有分区，则必须使所有权与新系统保持一致。

过程：根分区崩溃后进行恢复

1. 安装 SUSE Manager。不要挂载 `/var/spacewalk` 和 `/var/lib/pgsql` 分区。等待安装完成，然后继续下一步。
2. 关闭数据库：

```
rcpostgresql stop
```

3. 关闭服务：

```
spacewalk-service stop
```

4. 挂载 `/var/spacewalk` 和 `/var/lib/pgsql` 分区。
5. 还原备份 SUSE Manager中列出的目录。
6. 启动数据库：

```
rcpostgresql start
```

7. 启动 spacewalk 服务：

```
spacewalk-service start
```

SUSE Manager 现在应该可以正常运行，而不会丢失数据库或已同步的通道。

4.9. 数据库连接信息

可以通过在 `/etc/rhn/rhn.conf` 中添加或编辑以下变量来设置 SUSE Manager 数据库连接信息：

```
db_backend = postgresql
db_user = susemanager
db_password = susemanager
db_name = susemanager
db_host = localhost
db_port = 5432
db_ssl_enabled =
```

Chapter 5. 内容暂存

客户端使用暂存来预先下载软件包，然后再安装软件包。这样就可以在做好安排后立即开始安装软件包，从而减少维护时段占用的时间。

5.1. 启用内容暂存

您可以管理整个组织中的内容暂存。在 SUSE Manager Web UI 中，导航到**管理 › 组织**以查看可用组织的列表。单击某个组织的名称，然后选中启用暂存内容框以允许此组织中的客户端暂存软件包数据。

> 您必须以 SUSE Manager 管理员身份登录才能创建和管理组织。

也可以在命令提示符下通过编辑 `/etc/sysconfig/rhn/up2date` 并添加或编辑下面一行内容来启用暂存：

```
stagingContent=1
stagingContentWindow=24
```

`stagingContentWindow` 参数是以小时为单位的时间值，用于确定下载何时开始。它是距离安排的安装或更新时间的小时数。在此示例中，将在安装时间之前的 24 小时开始下载内容。下载开始时间取决于为系统选择的联系方法。指派的联系方法设置下一个 `mgr_check` 的执行时间。

下一次安排操作后，会自动下载但不安装软件包。将在安排的时间安装暂存的软件包。

5.2. 配置内容暂存

有两个参数用于配置内容暂存：

- `salt_content_staging_advance` 是内容暂存时段开始之前预先经过的一段时间，以小时为单位。 它是距离安装开始的小时数，经过这段时间后即可开始下载软件包。
- `salt_content_staging_window` 是内容暂存时段的持续时间，以小时为单位。 这是在安装开始之前客户端必须将软件包暂存的一段时间。

例如，如果 `salt_content_staging_advance` 设置为六小时，`salt_content_staging_window` 设置为两小时，则暂存时段在安装时间到来之前的六小时开始，并持续两小时。在安装开始之前的剩余四个小时内不会下载任何软件包。

如果您为 `salt_content_staging_advance` 和 `salt_content_staging_window` 设置相同的值，则可以在安装开始之前下载软件包。

在 `/usr/share/rhn/config-defaults/rhn_java.conf` 中配置内容暂存参数。

默认值：

- `salt_content_staging_advance: 8 小时`
- `salt_content_staging_window: 8 小时`

必须启用内容暂存才能让这些参数正常工作。

Chapter 6. 通道管理

通道是将软件包分组的一种方法。

在 SUSE Manager 中，通道分为基础通道和子通道，基础通道按操作系统类型、版本和体系结构分组，子通道与其相关的基础通道兼容。将客户端指派到基础通道后，该系统只能安装相关的子通道。以这种方式组织通道可确保在每个系统上仅安装兼容的软件包。

软件通道使用储存库来提供软件包。通道镜像 SUSE Manager 中的储存库，软件包名称和其他数据存储在 SUSE Manager 数据库中。您可以使用与某个通道关联的任意数量的储存库。然后可以通过让客户端订阅相应的通道，将这些储存库中的软件安装在客户端上。

客户端只能指派到一个基础通道。然后，客户端可以安装或更新与该基础通道及其任何子通道关联的储存库中的软件包。

SUSE Manager 提供了许多供应商通道，这些通道为您提供了运行 SUSE Manager 所需的一切。SUSE Manager 管理员和通道管理员拥有通道管理权限，他们可以创建和管理自己的自定义通道。如果您想在环境中使用自己的软件包，可以创建自定义通道。自定义通道可以用作基础通道，或者您也可以将它们与供应商基础通道相关联。

有关创建自定义通道的详细信息，请参见 **Administration › Custom-channels**。

6.1. 通道管理

默认情况下，任何用户都可以在系统中订阅通道。您可以使用 Web UI 对通道实施限制。

过程：限制订阅者对通道的访问权限

1. 在 SUSE Manager Web UI 中，导航到 **软件 › 通道列表**，并选择要编辑的通道。
2. 找到每个用户的订阅限制部分并选中只有您组织中的选定用户可以订阅此通道。单击 **[更新]** 保存更改。
3. 导航到订阅者选项卡，并根据需要选择或取消选择用户。

6.2. 删除通道

可以从命令提示符删除供应商软件通道。

有关删除自定义通道的信息，请参见 **Administration › Custom-channels**。

过程：删除供应商通道

1. 在 SUSE Manager Server 上的在命令提示符下，以 root 身份列出可用的供应商通道，并记下您要删除的通道：

```
mgr-sync list channels
```

2. 删除通道：

```
spacewalk-remove-channel -c <通道名称>
```

3. 同步以去除通道：

```
mgr-sync sync channel <通道名称>
```

6.3. 相关主题

- 有关如何手动删除通道的详细信息，请参见 **Common-workflows › Workflow-removing-channel**。

6.4. 自定义通道

自定义通道使您能够创建自己的软件包和储存库，然后可以使用这些软件包和储存库来更新您的客户端。它们还使您能够在环境中使用第三方供应商提供的软件。

本节提供有关如何创建、管理和删除自定义通道的更多细节。您必须拥有管理员特权才能创建和管理自定义通道。

6.4.1. 创建自定义通道和储存库

在创建自定义通道之前，请确定要将其关联到哪个基础通道，以及要为内容使用哪些储存库。

如果您需要将自定义软件包安装在客户端系统上，可以创建自定义子通道来管理它们。需要在 SUSE Manager Web UI 中创建通道，并为软件包创建储存库，然后将该通道指派到系统。

> 不要创建其中有软件包与客户端系统不兼容的子通道。

如果您要使用供应商提供的软件包，可以选择供应商通道作为基础通道。或者，选择无以将自定义通道设为基础通道。

过程：创建自定义通道

1. 在 SUSE Manager Web UI 中，导航到**软件 › 管理 › 通道**，然后单击 **[创建通道]**。
2. 在创建软件通道页面上，为您的通道命名（例如 `My Tools SLES 15 SP1 x86_64`）和标签（例如 `my-tools-sles15sp1-x86_64`）。 标签不能包含空格或大写字母。
3. 在父通道下拉菜单中选择相关的基础通道（例如 `SLE-Product-SLES15-SP1-Pool for x86_64`）。 确保为软件包选择兼容的父通道。
4. 在体系结构下拉菜单中选择适当的硬件体系结构（例如 `x86_64`）。
5. 根据环境的需要，在联系方法细节、通道访问控制和 GPG 字段中提供任何附加信息。
6. 单击 **[创建通道]**。

自定义通道有时需要额外的安全设置。许多第三方供应商使用 GPG 保护软件包。如果您想要在自定义通道中使用受 GPG 保护的软件包，需要信任用来为元数据签名的 GPG 密钥。然后，可以选中包含已签名的元数据？复

选框，以将软件包元数据与受信任的 GPG 密钥进行匹配。

如果远程通道和储存库已使用 GPG 密钥签名，则您可以导入并信任这些 GPG 密钥。例如，从 SUSE Manager Server 上的命令行执行 `spacewalk-repo-sync`：

```
/usr/bin/spacewalk-repo-sync -c <通道标签名称> -t yum
```

基础 `zypper` 调用将导入密钥（如果已提供）。Web UI 不提供此功能。

仅当您要镜像的储存库是以特殊方式设置的，并且储存库中的签名旁边提供了“key”时，才可以正常完成此操作。开放式构建服务（OBS）生成的所有储存库都是这种情况。对于其他储存库，需要完成特殊的准备步骤（参见下文！）。

> 当您创建新通道时，默认会选中启用 GPG 检查字段。如果您要将自定义软件包和应用程序添加到您的通道，请务必取消选中此字段，以便能够安装未签名的软件包。如果软件包来自不受信任的源，则禁用 GPG 检查会带来安全风险。

> 如果您正在注册传统的 Red Hat Enterprise Linux 7 或 SLES Expanded Support 7 客户端，有可能会看到未签名软件包的错误。有关详细信息，请参见 **Administration › Troubleshooting**。

仅当储存库是有效的软件储存库时，才能使用 Web UI 将其添加到 SUSE Manager。请提前检查是否提供了所需的储存库元数据。可以使用 `createrepo` 和 `reprepro` 等工具进行这种检查。`mgrpush` 可帮助您将单个 RPM 推送到通道，而无需创建储存库。有关详细信息，请参见 `createrepo_c` 和 `reprepro` 的手册页。

过程：添加软件储存库

1. 在 SUSE Manager Web UI 中，导航到**软件 › 管理 › 储存库**，然后单击 **[创建储存库]**。
2. 在创建储存库页面上，为该储存库指定标签（例如 `my-tools-sles15sp1-x86_64-repo`）。
3. 在储存库 URL 字段中，提供包含 `repodata` 文件的目录的路径（例如 file:///opt/mytools/）。可以在此字段中使用任何有效寻址协议。
4. 取消选中包含已签名的元数据？复选框。
5. 可选：如果您的储存库需要客户端证书身份验证，请填写 SSL 字段。
6. 单击 **[创建储存库]**。

仅当您要镜像的储存库中在签名旁边提供了“key”时，才能正常完成上述过程。OBS 生成的所有储存库都是这种情况，但其他不是由 OBS 提供的操作系统储存库并非如此。

如果您要使用的储存库不包含 GPG 密钥，您可以自己提供一个 GPG 密钥并手动将其导入密钥环。如果您使用 `gpg` 命令行工具将密钥导入 `/var/lib/spacewalk/gpgdir` 密钥环，将永久存储该密钥。即使清理了 chroot 环境，也会持久保存该密钥。

过程：使用 GPG 密钥创建软件储存库

1. 用于将密钥导入 pub 密钥环的 gpg 命令是：

```
gpg --keyring /var/lib/spacewalk/gpgdir  --import /path/to/gpg.key
gpg --edit-key <密钥 ID>
```

使用 `uyuni_suite`、`uyuni_component` 和 `uyuni_arch` 查询参数添加 Debian 非平面储存库。

`uyuni_suite`

是必需的。在 Debian 文档中，此参数也名为 `distribution`。使用此参数可以指定 apt 源。如果不提供此参数，则会使用原始方法。如果该参数以 `/` 结尾，则会将储存库标识为平面储存库。

`uyuni_component`

是可选的。此参数只能指定一个组件。无法列出组件。一个 apt 源项允许指定多个组件，但对于 Uyuni 无法做到这一点。对此，您必须为每个组件创建单独的储存库。

`uyuni_arch`

是可选的。如果将其省略，则会使用 SQL 查询为数据库中的通道计算体系结构名称。如果`uyuni_arch`与通道体系结构不匹配（有时体系结构命名不明确），请显式指定此参数。

下面提供了一些示例：

表格 2. Debian 非平面储存库映射

类型	源行/URL
apt 源行	`deb` https://pkg.jenkins.io/debian-stable `binary/`
URL 映射	https://pkg.jenkins.io/debian-stable?uyuni_suite=binary/
apt 源行	`deb` https://deb.debian.org/debian/dists `stable main`
URL 映射	https://deb.debian.org/debian/dists?uyuni_suite=stable&uyuni_component=main

在此处查找有关 Debian 储存库定义格式的背景信息。此信息基于 https://wiki.debian.org/DebianRepository/Format#Overview。

储存库定义格式如下：

```
deb URI 套件 [组件 1] [组件 2] [...]
```

例如：

```
deb https://deb.debian.org/debian/dists stable main
```

或

```
deb https://pkg.jenkins.io/debian-stable binary/
```

对于每一对套件和组件，规范定义了一个根据基 URL + 套件 + 组件计算的不同 URL。

过程：将储存库指派到通道

1. 通过导航到**软件 › 管理 › 通道**，单击新建的自定义通道的名称，然后导航到储存库选项卡，将新储存库指派到自定义通道。
2. 确保选中您要指派到通道的储存库，然后单击 **[更新储存库]**。
3. 导航到同步选项卡，然后单击 **[立即同步]** 立即同步。有关通道同步的详细信息，请参见下文。

过程：将自定义通道添加到激活密钥

1. 在 SUSE Manager Web UI 中，导航到**系统 › 激活密钥**，然后选择要将自定义通道添加到的密钥。
2. 在细节选项卡上的子通道列表中，选择要关联的通道。 如果需要，您可以选择多个通道。
3. 单击 **[更新激活密钥]**。

6.4.2. 自定义通道同步

为了避免错过重要更新，SUSE 建议通过远程储存库更改来使您的自定义通道保持最新。

系统默认不会自动同步自定义通道。为了确保自定义通道保持最新状态，您需要：

- 通过导航到同步选项卡并单击 **[立即同步]** 来手动同步该通道。
- 在储存库选项卡中设置自动同步日程安排。

您也可以为创建的所有自定义通道启用自动同步。要实现此目的，请在 `/etc/rhn/rhn.conf` 中进行如下设置：

```
java.unify_custom_channel_management = 1
```

启用此属性后，系统将会自动执行一次同步：

- 在 UI 中或者使用 `spacewalk-common-channels` 将储存库添加到通道后
- 在执行日常任务 `mgr-sync-refresh-default` 的过程中，这将同步您的所有自定义通道和供应商通道。

该过程开始后，可通过多种方式检查通道是否已完成同步：

- 在 SUSE Manager Web UI 中，导航到**管理 › 安装向导**，然后选择产品选项卡。 产品同步时，此对话框将为每个产品显示一个完成栏。
- 在 SUSE Manager Web UI 中，导航到**软件 › 管理 › 通道**，然后单击与储存库关联的通道。 导航到**储存库 › 同步**选项卡。储存库名称旁边会显示同步状态。
- 在命令提示符下检查同步日志文件：

  ```
  tail -f /var/log/rhn/reposync/<channel-label>.log
  ```

  每个子通道在同步过程中会生成自身的日志。您需要检查所有基础通道和子通道日志文件，以确保同步完成。

6.4.3. 将软件包和补丁添加到自定义通道

如果您创建新的自定义通道但未从现有通道克隆，则创建的通道不包含任何软件包或补丁。可以使用 SUSE Manager Web UI 添加所需的软件包和补丁。

自定义通道只能包含克隆的或者自定义的软件包或补丁，并且这些软件包或补丁必须与通道的基础体系结构相匹配。添加到自定义通道的补丁必须适用于通道中的软件包。

过程：将软件包添加到自定义通道

1. 在 SUSE Manager Web UI 中，导航到**软件 › 管理 › 通道**，然后转到软件包选项卡。
2. 可选：通过导航到列出/去除选项卡查看当前包含在通道中的所有软件包。
3. 通过导航到添加选项卡将新软件包添加到通道。
4. 选择要为其提供软件包的父通道，然后单击 **[查看软件包]** 以填充列表。
5. 检查要添加到自定义通道的软件包，然后单击 **[添加软件包]**。
6. 如果您觉得选择合适，请单击 **[确认添加]** 以将软件包添加到通道。
7. 可选：可以通过导航到**软件 › 管理 › 通道**，然后转到**软件包 › 比较**选项卡，将当前通道中的软件包与其他通道中的软件包进行比较。 要使两个通道相同，请单击 **[合并差异]** 按钮，然后解决任何冲突。

过程：将补丁添加到自定义通道

1. 在 SUSE Manager Web UI 中，导航到**软件 › 管理 › 通道**，然后转到补丁选项卡。
2. 可选：通过导航到列出/去除选项卡查看当前包含在通道中的所有补丁。
3. 通过导航到添加选项卡，然后选择要添加的补丁类型，将新补丁添加到通道。
4. 选择要为其提供补丁的父通道，然后单击 **[浏览关联补丁]** 以填充列表。

5. 检查要添加到自定义通道的补丁，然后单击 **[确认]**。
6. 如果您觉得选择合适，请单击 **[确认]** 以将补丁添加到通道。

6.4.4. 管理自定义通道

SUSE Manager 管理员和通道管理员可以更改或删除任何通道。

要授予其他用户更改或删除通道的权限，请导航到**软件 › 管理 › 通道**，然后选择要编辑的通道。导航到管理者选项卡，并选中要向其授予权限的用户。单击 **[更新]** 以保存更改。

> 如果您删除某个已指派到一组客户端的通道，与已删除通道关联的任何客户端的通道状态将立即更新。这是为了确保在储存库文件中准确反映所做的更改。

无法使用 Web UI 删除 SUSE Manager 通道。只能删除自定义通道。

过程：删除自定义通道

1. 在 SUSE Manager Web UI 中，导航到**软件 › 管理 › 通道**，然后选择要删除的通道。
2. 单击 **[删除软件通道]**。
3. 在删除通道页面上，检查您要删除的通道的细节，然后选中取消订阅系统复选框，以从任何可能仍已订阅的系统中去除该自定义通道。
4. 单击 **[删除通道]**。

删除通道时，不会自动去除其中的软件包。您无法更新其通道已被删除的软件包。

可以在 SUSE Manager Web UI 中删除与通道没有关联的软件包。导航到**软件 › 管理 › 软件包**，选中要去除的软件包，然后单击 **[删除软件包]**。

Chapter 7. 内容生命周期管理

内容生命周期管理允许您在更新生产客户端之前自定义和测试软件包。如果您需要在有限的维护时段内应用更新，此功能将特别有用。

内容生命周期管理允许您选择软件通道作为源、根据环境的需要调整软件通道，并在安装到生产客户端之前对其进行全面的测试。

虽然您无法直接修改供应商通道，但可以克隆它们，然后通过添加或去除软件包和自定义补丁来修改克隆版本。可以将这些克隆的通道指派到测试客户端，以确保它们按预期工作。

> 默认情况下，克隆的供应商通道与原始供应商通道一致并会自动选择依赖项。您可以在 `/etc/rhn/rhn.conf` 中添加以下选项来禁止自动为克隆的通道选择依赖项：
>
> ```
> java.cloned_channel_auto_selection = false
> ```

然后，当所有测试都通过后，您可以将克隆的通道升级为生产服务器。

此功能是通过一系列环境实现的，软件通道在其生命周期内可以在这些环境之间转移。大多数环境生命周期至少包括测试和生产环境，但您可以创建任意所需数量的环境。

本章介绍基本的内容生命周期过程以及可用的过滤器。有关更具体的示例，请参见 **Administration › Content-lifecycle-examples**。

7.1. 创建内容生命周期项目

要设置内容生命周期，需要从一个项目开始。该项目定义软件通道源、用于查找软件包的过滤器，以及构建环境。

过程：创建内容生命周期项目

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 项目**并单击 **[创建项目]**。
2. 在 标签字段中输入项目的标签。 标签字段仅接受小写字母、数字、句点、连字符和下划线。
3. 在名称字段中输入项目的描述性名称。
4. 单击 **[创建]** 按钮以创建项目并返回项目页面。
5. 单击 **[挂接/分离源]**。
6. 在源对话框中选择源类型，然后选择项目的基础通道。 此时会显示所选基础通道的可用子通道，包括有关通道是必需通道还是建议通道的信息。
7. 选中所需的子通道，然后单击 **[保存]** 返回项目页面。 您选择的软件通道现在应会显示出来。
8. 单击 **[挂接/分离过滤器]**。
9. 在筛选器对话框中，选择要挂接到项目的过滤器。 要创建新过滤器，请单击 **[创建新过滤器]**。
10. 单击 **[添加环境]**。

11. 在环境生命周期对话框中，为第一个环境指定名称、标签和说明，然后单击 **[保存]**。 标签字段仅接受小写字母、数字、句点、连字符和下划线。
12. 继续创建环境，直到为整个生命周期创建了所有环境。 可以选择环境在生命周期中的顺序，方法是在创建某个环境时在在前面插入字段中选择该环境。

7.2. 过滤器类型

SUSE Manager 允许您创建各种类型的过滤器来控制用于构建项目的内容。使用过滤器可以选择要在构建中包含或排除哪些软件包。例如，可以排除所有内核软件包，或仅包含某些软件包的特定发行版。

支持的过滤器为：

- 软件包过滤
  - 按名称
  - 按名称、纪元、版本、发行版和体系结构
  - 按提供的名称
- 补丁过滤
  - 按建议名称
  - 按建议类型
  - 按摘要
  - 按关键字
  - 按日期
  - 按受影响的软件包
- 模块
  - 按流

> 在内容过滤期间不会解析软件包依赖项。

可以将多个匹配器与过滤器配合使用。哪些匹配器可用取决于所选的过滤器类型。

可用的匹配器为：

- 包含
- 匹配（必须采用正则表达式形式）
- 等于
- 大于
- 大于或等于
- 低于或等于

- 低于
- 高于或等于

7.2.1. 过滤器规则参数

每个过滤器都有一个规则参数，可将此参数设置为允许或拒绝。过滤器的处理方式如下：

- 如果某个软件包或补丁满足拒绝过滤器的条件，则从结果中排除它。
- 如果某个软件包或补丁满足允许过滤器的条件，则将它包含在结果中（即使它已由拒绝过滤器排除）。

当您想要使用一般的拒绝过滤器来排除大量软件包或补丁，并想要使用特定的允许过滤器来“挑选”特定的软件包或补丁时，此行为很有用。

> 内容过滤器在您的组织中是全局性的，并可以在项目之间共享。

> 如果您的项目已包含构建的源，当您添加环境时，该环境中会自动填充现有内容。内容是从周期中的前一个环境（如果有）提取的。如果前一个环境不存在，则将内容留空，直到再次构建了项目源。

7.3. 过滤器模板

为了帮助为某些常见方案创建过滤器，SUSE Manager 提供了过滤器模板。应用这些模板有助于提前创建一组针对特定用例定制的过滤器。

本节介绍可用的模板及其用法。

7.3.1. 根据 SUSE 产品在线增补

在包含在线增补的项目中，必须排除未来的常规内核软件包，以便仅将在线补丁软件包作为更新提供给客户端。另一方面，仍然必须包含已安装的常规内核软件包以保持系统完整性。

应用此模板会创建三个所需的过滤器来实现以下行为：

- 允许其中包含与基础内核版本相同的 `kernel-default` 软件包的补丁
- 拒绝其中包含 `reboot_suggested` 关键字的补丁
- 拒绝其中包含带有名称 `installhint(reboot-needed)` 的软件包的补丁

有关如何设置在线增补项目的详细信息，请参见 administration:content-lifecycle-examples.pdf。

过程：应用模板

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 过滤器**并单击 **[创建过滤器]**。
2. 在对话框中单击 **[使用模板]**。输入将相应地更改。

3. 在前缀字段中键入名称前缀。此值将添加到模板创建的每个过滤器的名称前面。如果在项目上下文中应用模板，则此字段中会预先填充项目标签。
4. 在模板字段中，选择根据 SUSE 产品在线增补。
5. 在产品字段中，选择要为其设置在线增补的产品。
6. 在内核字段中，从所选产品的可用版本列表中选择一个内核版本。拒绝后续常规内核补丁的过滤器将基于此版本。
7. 单击 **[保存]** 以创建过滤器。
8. 导航到**内容生命周期 › 项目**并选择您的项目。
9. 单击 **[挂接/分离过滤器]**。
10. 选择具有指定前缀的三个过滤器，然后单击 **[保存]**。

7.3.2. 根据系统在线增补

如果您想要根据特定已注册系统中安装的内核版本设置在线增补项目，可以使用根据系统在线增补模板。

应用此模板会创建三个所需的过滤器来实现以下行为：

- 允许其中包含与基础内核版本相同的 `kernel-default` 软件包的补丁
- 拒绝其中包含 `reboot_suggested` 关键字的补丁
- 拒绝其中包含带有名称 `installhint(reboot-needed)` 的软件包的补丁

有关如何设置在线增补项目的详细信息，请参见 administration:content-lifecycle-examples.pdf。

过程：应用模板

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 过滤器**并单击 **[创建过滤器]**。
2. 在对话框中单击 **[使用模板]**。输入将相应地更改。
3. 在前缀字段中键入名称前缀。此值将添加到模板创建的每个过滤器的名称前面。如果在项目上下文中应用模板，则此字段中会预先填充项目标签。
4. 在模板字段中，选择根据特定系统在线增补。
5. 在系统字段中，从列表中选择一个系统，或键入系统名称以缩小选项的范围。
6. 在内核字段中，从所选系统上安装的版本列表中选择一个内核版本。拒绝后续常规内核补丁的过滤器将基于此版本。
7. 单击 **[保存]** 以创建过滤器。
8. 导航到**内容生命周期 › 项目**并选择您的项目。
9. 单击 **[挂接/分离过滤器]**。
10. 选择具有指定前缀的三个过滤器，然后单击 **[保存]**。

7.3.3. 含默认值的 AppStream 模块

如果您想要在项目中包含模块化储存库中提供的所有可用模块，可以使用此过滤器模板自动添加这些模块。

应用后，此模板将为每个模块及其默认流创建一个 AppStream 过滤器。

如果从项目的页面完成此过程，则过滤器将自动添加到项目。否则，创建的过滤器可能会列在**内容生命周期 › 过滤器**中，并根据需要添加到任何项目。

可以编辑每个过滤器以选择不同的模块流，或去除所有这些过滤器以从目标储存库中排除该模块。

由于并非所有模块流都相互兼容，因此更改单个流可能会导致无法成功解析模块化依赖关系。如果发生这种情况，项目细节页面中的过滤器窗格会显示描述问题的错误，并且在选择的所有模块都兼容之前，构建按钮将会禁用。

自 Red Hat Enterprise Linux 9 起，模块便不再具有任何定义的默认流。因此，对 Red Hat Enterprise Linux 9 源使用此模板将不会有任何效果。

有关如何使用内容生命周期管理设置 AppStream 储存库的详细信息，请参见 administration:content-lifecycle-examples.pdf。

过程：应用模板

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 项目**，然后选择您的项目。
2. 在过滤器部分，单击 **[挂接/分离过滤器]**，然后单击 **[创建新过滤器]**。
3. 在对话框中单击 **[使用模板]**。输入将相应地更改。
4. 在前缀字段中键入名称前缀。此值将添加到模板创建的每个过滤器的名称前面。如果在项目上下文中应用模板，则此字段中会预先填充项目标签。
5. 在模板字段中，选择`含默认值的 AppStream 模块`。
6. 在通道字段中，选择一个模块化通道以从中获取模块。此下拉列表中仅显示模块化通道。
7. 单击 **[保存]** 以创建过滤器。
8. 滚动到过滤器部分以查看新挂接的 AppStream 过滤器。
9. 可以编辑/去除任何一个过滤器以根据您的需要定制项目。

7.4. 构建内容生命周期项目

创建项目、定义环境、挂接源和过滤器后，可以首次构建项目。

构建过程会将过滤器应用于挂接的源，并将过滤器克隆到项目中的第一个环境。

可以使用相同的供应商通道作为多个内容项目的源。在这种情况下，SUSE Manager 不会为每个克隆的通道创建新的补丁克隆版本，而是在所有克隆的通道之间共享一个补丁克隆版本。如果供应商修改了某个补丁（例如，撤回了该补丁，或者更改了补丁中的软件包），则这可能会导致问题。当您构建某个内容项目时，默认情况下，共享克隆补丁的所有通道将与原始通道同步，即使这些共享通道位于内容项目的其他环境中，或者位于您

的组织的其他内容项目通道中，也是如此。可以通过在组织设置中关闭自动补丁同步来更改此行为。要在以后为共享补丁的所有通道手动同步补丁，请导航到**软件 › 管理 › 通道**，单击要同步的通道，然后导航到同步子选项卡。即使手动同步补丁，也会影响共享补丁的所有组织通道。

过程：构建内容生命周期项目

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 项目**，然后选择您要构建的项目。

   在构建项目前，请确保环境可用。

2. 查看挂接的源和过滤器，然后单击 **[构建]**。
3. 提供版本消息以描述此构建中的更改或更新。
4. 可以在环境生命周期部分监视构建进度。

构建完成后，环境版本号将会加 1，可将构建的源（例如软件通道）指派到您的客户端。

7.5. 升级环境

构建项目后，可将构建的源按顺序升级到环境。

过程：升级环境

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 项目**，然后选择您要处理的项目。
2. 在环境生命周期部分，找到要升级到其后继版本的环境，然后单击 **[升级]**。
3. 可以在环境生命周期部分监视构建进度。

7.6. 将客户端指派到环境

当您构建和升级内容生命周期项目时，SUSE Manager 会创建一个软件通道树。要将客户端添加到环境，请使用客户端的系统细节页面中的**软件 › 软件通道**将基础通道和子软件通道指派到客户端。

新添加的克隆通道不会自动指派到客户端。如果您添加或升级了源，则需要手动检查并更新您的通道指派。

在将来的版本中，自动指派会添加到 SUSE Manager。

7.7. 内容生命周期管理示例

本节提供了一些常见示例来说明如何使用内容生命周期管理。请使用这些示例来构建您自己的个性化实现。

7.7.1. 为每月增补周期创建项目

每月增补周期的示例项目包括：

- 创建一个按日期过滤器
- 将过滤器添加到项目
- 将过滤器应用于新项目构建
- 从项目中排除补丁
- 在项目中包含补丁

7.7.1.1. 创建一个按日期过滤器

按日期过滤器排除指定日期之后发布的所有补丁。此过滤器对于遵循每月增补周期的内容生命周期项目很有用。

过程：创建按日期过滤器

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 过滤器**并单击 **[创建过滤器]**。
2. 在过滤器名称字段中键入过滤器的名称。 例如，按日期排除补丁。
3. 在过滤器类型字段中选择补丁（发布日期）。
4. 在匹配器字段中，已自动选择晚于或等于。
5. 选择日期和时间。
6. 单击 **[保存]**。

7.7.1.2. 将过滤器添加到项目

过程：将过滤器添加到项目

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 项目**并从列表中选择一个项目。
2. 单击 **[挂接/分离过滤器]** 链接以查看所有可用的过滤器
3. 选择新的按日期排除补丁过滤器。
4. 单击 **[保存]**。

7.7.1.3. 将过滤器应用于新项目构建

新过滤器已添加到过滤器列表，但仍然需要将其应用于项目。要应用过滤器，需要构建第一个环境。

过程：使用过滤器

1. 单击 **[构建]** 以构建第一个环境。
2. 可选：添加消息。 可以使用消息来帮助跟踪构建历史记录。
3. 在测试服务器上使用新通道来检查过滤器是否正常工作。
4. 单击 **[升级]** 将内容移到下一个环境。 如果您有大量过滤器，或者过滤器非常复杂，则构建过程需要较长时间。

7.7.1.4. 从项目中排除补丁

测试可以帮助您发现问题。如果发现问题，请排除按日期过滤器之前发布的有问题补丁。

过程：排除补丁

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 过滤器**并单击 **[创建过滤器]**。
2. 在过滤器名称字段中输入过滤器的名称。 例如，`排除 openjdk 补丁`。
3. 在过滤器类型字段中选择补丁（建议名称）。
4. 在匹配器字段中选择等于。
5. 在建议名称字段中键入建议名称。 例如，`SUSE-15-2019-1807`。
6. 单击 **[保存]**。
7. 导航到**内容生命周期 › 项目**并选择您的项目。
8. 单击 **[挂接/分离过滤器]** 链接，选择`排除 openjdk 补丁`，然后单击 **[保存]**。

当您使用 **[构建]** 按钮重构建项目时，新过滤器将与前面添加的按日期过滤器一起使用。

7.7.1.5. 在项目中包含补丁

此示例假设您收到了一条安全警报。当前工作月刚过几天，发布了一个重要的安全补丁。新补丁的名称是`SUSE-15-2019-2071`。您需要将此新补丁包含在您的环境中。

> 允许过滤器规则会覆盖拒绝过滤器规则的排除功能。有关详细信息，请参见 **Administration › Content-lifecycle**。

过程：在项目中包含补丁

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 过滤器**并单击 **[创建过滤器]**。
2. 在过滤器名称字段中键入过滤器的名称。 例如，`包含内核安全修复`。
3. 在过滤器类型字段中选择补丁（建议名称）。
4. 在匹配器字段中选择等于。
5. 在建议名称字段中键入 `SUSE-15-2019-2071`，然后选中允许。
6. 单击 **[保存]** 以存储该过滤器。
7. 导航到**内容生命周期 › 项目**并从列表中选择您的项目。
8. 单击 **[挂接/分离过滤器]**，然后选择包含内核安全补丁。
9. 单击 **[保存]**。
10. 单击 **[构建]** 以重构建环境。

7.7.2. 更新现有的每月增补周期

每月增补周期完成后，您可以更新下个月的增补周期。

过程：更新每月增补周期

1. 在按日期字段中，将过滤器的日期更改为下个月。 或者，创建一个新过滤器并更改项目的指派。
2. 检查是否可以将 SUSE-15-2019-1807 的排除过滤器从项目中分离。 可能有一个新补丁可以修复此问题。
3. 分离前面添加的允许过滤器。 默认已包含该补丁。
4. 重构建项目以创建包含下个月补丁的新环境。

7.7.3. 使用在线增补增强项目

本节介绍如何设置过滤器以创建可在线增补的环境。

> 当您准备使用在线增补时，需要注意一些重要事项
>
> - 永远只在您的系统上使用一个内核版本。 在线增补软件包与特定内核一起安装。
> - 在线增补更新作为一个补丁交付。
> - 后续会安装一系列新在线增补内核的每个内核补丁会显示需要重引导标志。 这些内核补丁附带在线增补工具。安装这些补丁后，需要在下一年开始之前至少重引导系统一次。
> - 仅安装与已安装内核版本匹配的在线补丁更新。
> - 在线补丁作为独立补丁提供。 您必须排除内核版本高于当前安装版本的所有常规内核补丁。

7.7.3.1. 排除内核版本较高的软件包

在此示例中，您将使用 SUSE-15-2019-1244 补丁更新您的系统。此补丁包含 kernel-default-4.12.14-150.17.1-x86_64。

需要排除所有包含较高版本 kernel-default 的补丁。

过程：排除内核版本较高的软件包

1. 在 SUSE Manager Web UI 中，导航到**内容生命周期 › 过滤器**并单击 **[创建过滤器]**。
2. 在过滤器名称字段中键入过滤器的名称。 例如，排除内核版本大于 4.12.14-150.17.1 的软件包。
3. 在过滤器类型字段中选择补丁（包含软件包）。
4. 在匹配器字段中选择版本大于。
5. 在软件包名称字段中键入 kernel-default。
6. 将纪元字段留空。
7. 在版本字段中键入 4.12.14。

8. 在发行版字段中键入 150.17.1。
9. 单击 [**保存**] 以存储该过滤器。
10. 导航到**内容生命周期 › 项目**并选择您的项目。
11. 单击 [**挂接/分离过滤器**]。
12. 选择排除内核版本大于 4.12.14-150.17.1 的软件包，然后单击 [**保存**]。

单击 [**构建**] 后，会创建一个新环境。新环境包含版本不高于所安装版本的所有内核补丁。

所有内核版本更高的内核补丁都将被去除。只要在线增补内核不是发行系列中的第一个，它们就仍然可用。

可以使用过滤器模板自动完成此过程。有关如何应用在线增补过滤器模板的详细信息，请参见 administration:content-lifecycle.pdf。

7.7.4. 切换到在线增补的新内核版本

特定内核版本的在线增补仅可使用一年。一年后，您必须更新系统上的内核。执行以下环境更改：

过程：切换到新内核版本

1. 确定要升级到哪个内核版本。 例如：4.12.14-150.32.1
2. 创建新的内核版本过滤器。
3. 分离先前创建的过滤器**排除内核版本大于 4.12.14-150.17.1 的软件包**并挂接新过滤器。

单击 [**构建**] 以重构建环境。新环境包含版本不高于所选新内核版本的所有内核补丁。使用这些通道的系统具有可供安装的内核更新。您需要在系统执行升级后重引导系统。新内核的有效期为一年。在当年安装的所有软件包与当前在线增补内核过滤器匹配。

7.7.5. AppStream 过滤器

如果您使用的是 Red Hat Enterprise Linux 8 或更高版本的客户端，则无法直接从模块化储存库（例如 Red Hat Enterprise Linux AppStream 储存库）执行软件包操作，例如安装或升级。您可以使用 AppStream 过滤器将模块化储存库转换为常规储存库。为此，该过滤器会将软件包保留在储存库中，并除去模块元数据。可以在 SUSE Manager 中像使用常规储存库一样使用转换后的储存库。

AppStream 过滤器将选择要包含在目标储存库中的单个模块流。您可以添加多个过滤器来选择多个模块流。

如果您不在 CLM 项目中使用 AppStream 过滤器，则模块化源中的模块元数据将保持不变，并且目标储存库包含相同的模块元数据。只要在 CLM 项目中至少启用一个 AppStream 过滤器，所有目标储存库就会转换为常规储存库。

在某些情况下，您可能想要构建常规储存库，而不包含任何模块的软件包。要实现此目的，请使用匹配器无（禁用模块化）添加 AppStream 过滤器。这会在目标储存库中禁用所有模块。此设置非常适合用于 Red Hat Enterprise Linux 9 客户端，这种客户端大多数模块的默认版本均已包含在作为常规储存库提供的 AppStream

储存库中。

要使用 AppStream 过滤器，需要一个包含模块化储存库（例如 `Red Hat Enterprise Linux AppStream`）的 CLM 项目。在开始之前，请确保包含所需的模块作为源。

过程：使用 AppStream 过滤器

1. 在 SUSE Manager Web UI 中，导航到您的 Red Hat Enterprise Linux 8 或 9 CLM 项目。 确保已包含项目的 AppStream 通道。
2. 单击 **[创建过滤器]** 并使用以下参数：
   - 在过滤器名称字段中键入新过滤器的名称。
   - 在过滤器类型字段中选择模块（流）。
   - 在匹配器字段中选择等于。
   - 在模块名称字段中键入模块名称。 例如 `postgresql`。
   - 在流字段中键入所需流的名称。 例如 `10`。如果将此字段留空，则会选择模块的默认流。
3. 单击 **[保存]** 以创建新过滤器。
4. 导航到**内容生命周期 › 项目**并选择您的项目。
5. 单击 **[挂接/分离过滤器]**，选择您的新 AppStream 过滤器，然后单击 **[保存]**。

可以使用创建/编辑过滤器表单中的浏览功能从模块化通道的可用模块流列表中选择一个模块。

过程：浏览可用模块流

1. 在 SUSE Manager Web UI 中，导航到您的 Red Hat Enterprise Linux 8 或 9 CLM 项目。 确保已包含项目的 AppStream 通道。
2. 单击 **[创建过滤器]** 并使用以下参数：
   - 在过滤器名称字段中键入新过滤器的名称。
   - 在过滤器类型字段中选择模块（流）。
   - 在匹配器字段中选择等于。
3. 单击浏览可用模块以查看所有模块化通道。
4. 选择一个通道以浏览模块和流：
   - 在模块名称字段中，开始键入要搜索的模块名称，或者从列表中选择。
   - 在流字段中，开始键入要搜索的流名称，或者从列表中选择。

> 只能在浏览模块时选择通道。选定的通道不会与过滤器一起保存，并且不会对 CLM 过程产生任何影响。

您可以为要包含在目标储存库中的任何其他模块流创建额外的 AppStream 过滤器。会自动包含选定流所依赖的任何模块流。

> 请小心不要指定有冲突的、不兼容的或缺失的模块流。例如，从同一个模块中选择两个流是无效的。

过程：禁用模块化

1. 在 SUSE Manager Web UI 中，导航到您的 Red Hat Enterprise Linux 8 或 9 CLM 项目。 确保已包含项目的 AppStream 通道。
2. 单击 **[创建过滤器]** 并使用以下参数：
   - 在过滤器名称字段中键入新过滤器的名称。
   - 在过滤器类型字段中选择模块（流）。
   - 在匹配器字段中选择无（禁用模块化）。
3. 单击 **[保存]** 以创建新过滤器。
4. 导航到**内容生命周期 › 项目**并选择您的项目。
5. 单击 **[挂接/分离过滤器]**，选择您的新 AppStream 过滤器，然后单击 **[保存]**。

这样会有效从目标储存库中去除模块元数据，并排除属于模块的所有软件包。

当您使用 Web UI 中的 **[构建]** 按钮构建 CLM 项目时，目标储存库是不包含任何模块的常规储存库，其中包含来自选定模块流的软件包。

> 在 Red Hat Enterprise Linux 8 项目中完全禁用模块化可能导致环境存在缺陷，因为在 Red Hat Enterprise Linux 8 中，某些模块对于系统的健康运行是不可或缺的。

Chapter 8. 断开连接的设置

无法将 SUSE Manager 连接到互联网时，您可以在断开连接的环境中使用它。

在 SUSE Linux Enterprise 15 和更高版本上可以使用储存库镜像工具 (RMT)。RMT 取代了订阅管理工具 (SMT)，后者在较旧的 SUSE Linux Enterprise 安装中可用。

在断开连接的 SUSE Manager 设置中，RMT 或 SMT 使用外部网络连接到 SUSE Customer Center。所有软件通道和储存库会同步到可卸存储设备。然后可以使用该存储设备更新断开连接的 SUSE Manager 安装。

此设置可让您的 SUSE Manager 安装保留在断开连接的脱机环境中。

> 您的 RMT 或 SMT 实例必须用于直接管理 SUSE Manager Server。它不能用于管理级联的另一个 RMT 或 SMT 实例。

有关 RMT 的详细信息，请参见 https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-rmt.html。

8.1. 同步 RMT

可以在 SUSE Linux Enterprise 15 安装中使用 RMT 来管理运行 SUSE Linux Enterprise 12 或更高版本的客户端。

我们建议您为每个 SUSE Manager 安装设置一个专用 RMT 实例。

过程：设置 RMT

1. 在 RMT 实例上安装 RMT 软件包：

```
zypper in rmt-server
```

2. 使用 YaST 配置 RMT：

```
yast2 rmt
```

3. 按照提示完成安装。

有关设置 RMT 的详细信息，请参见 https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-rmt.html。

过程：将 RMT 与 SCC 同步

1. 在 RMT 实例上，列出您的组织可用的所有产品和储存库：

```
rmt-cli products list --all
rmt-cli repos list --all
```

2. 同步您的组织可用的所有更新：

```
rmt-cli sync
```

还可以使用 systemd 将 RMT 配置为定期同步。

3. 启用所需的产品。 例如，要启用 SLES 15，请运行以下命令：

```
rmt-cli product enable sles/15/x86_64
```

4. 将已同步的数据导出到可卸存储。 在此示例中，存储媒体的挂载位置为 `/mnt/usb`：

```
rmt-cli export data /mnt/usb
```

5. 将已启用的储存库导出到可卸存储：

```
rmt-cli export settings /mnt/usb
rmt-cli export repos /mnt/usb
```

确保将外部存储挂载到 RMT 用户可写的目录。可以在 `/etc/rmt.conf` 的 `cli` 部分中更改 RMT 用户设置。

8.2. 同步 SMT

SMT 已随附在 SUSE Linux Enterprise 12 中，可用于管理运行 SUSE Linux Enterprise 10 或更高版本的客户端。

SMT 要求您在 SMT 实例上创建一个本地镜像目录以同步储存库和软件包。

有关安装和配置 SMT 的更多细节，请参见 https://documentation.suse.com/sles/12-SP5/html/SLES-all/book-smt.html。

过程：将 SMT 与 SCC 同步

1. 在 SMT 实例上，创建一个数据库替换文件：

```
smt-sync --createdbreplacementfile /tmp/dbrepl.xml
```

2. 将已同步的数据导出到可卸存储。 在此示例中，存储媒体的挂载位置为 `/mnt/usb`：

```
smt-sync --todir /mnt/usb
smt-mirror --dbreplfile /tmp/dbrepl.xml --directory /mnt/usb \
        --fromlocalsmt -L /var/log/smt/smt-mirror-export.log
curl https://scc.suse.com/suma/product_tree.json -o /mnt/usb/product_tree.json
```

> 确保将外部存储挂载到 RMT 用户可写的目录。可以在 `/etc/smt.conf` 中更改 SMT 用户设置。

8.3. 必需通道

需要启用相应的 SUSE Manager 客户端工具通道，才能使 SUSE Manager 能够同步给定的通道。如果未启用这些通道，SUSE Manager 可能无法检测到该产品。

运行以下命令启用这些必需的通道：

SLES 12 和基于它的产品，例如 SLES for SAP 或 SLE HPC

RMT：`rmt-cli products enable sle-manager-tools/12/x86_64`

SMT：`smt repos -p sle-manager-tools,12,x86_64`

SLES 15 和基于它的产品，例如 SLES for SAP 或 SLE HPC

RMT：`rmt-cli products enable sle-manager-tools/15/x86_64`

SMT：`smt repos -p sle-manager-tools,15,x86_64`

然后镜像通道并导出。

可以启用其他发行套件或体系结构。有关启用要镜像的产品通道或储存库的详细信息，请参见文档：

RMT

https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-rmt-mirroring.html#sec-rmt-mirroring-enable-disable

SMT

https://documentation.suse.com/sles/12-SP5/single-html/SLES-smt/index.html#smt-mirroring-manage-domirror

8.4. 同步已断开连接的服务器

如果您有加载了 SUSE Customer Center 数据的可卸媒体，可以使用它来同步已断开连接的服务器。

过程：同步已断开连接的服务器

1. 将可卸媒体设备挂载到 SUSE Manager 服务器。 在此例子中，挂载点是 `/media/disk`。
2. 打开 `/etc/rhn/rhn.conf`，并通过添加或编辑下面一行内容来定义挂载点：

```
server.susemanager.fromdir = /media/disk
```

3. 重启动 Tomcat 服务：

```
systemctl restart tomcat
```

4. 刷新本地数据：

```
mgr-sync refresh
```

5. 执行同步：

```
mgr-sync list channels
mgr-sync add channel channel-label
```

用于同步的可御磁盘必须始终在同一挂载点上可用。如果未挂载存储媒体，请不要触发同步，否则会导致数据损坏。

请注意，如果设置了 `server.susemanager.fromdir`，SUSE Manager 将无法检查 SUSE Customer Center 身份凭证是否有效。相反，系统会显示一个警告信号，而不执行 SCC 联机检查。

Chapter 9. 管理磁盘空间

磁盘空间不足可能会对 SUSE Manager 数据库和文件结构造成严重影响，在某些情况下，这种影响不可恢复。

SUSE Manager 会监视某些目录的可用磁盘空间。您可以修改受监视的目录和创建的警告。所有设置都在 `/etc/rhn/rhn.conf` 配置文件中配置。

当某个受监视目录的可用空间低于警告阈值时，会向配置的电子邮件地址发送一条消息，并在登录页面顶部显示一条通知。

9.1. 受监视的目录

SUSE Manager 默认监视以下目录：

- `/var/lib/pgsql`
- `/var/spacewalk`
- `/var/cache`
- `/srv`

您可以使用 `spacecheck_dirs` 参数更改受监视的目录。可以指定多个目录并用空格将其分隔。

例如：

```
spacecheck_dirs = /var/lib/pgsql /var/spacewalk /var/cache /srv
```

9.2. 阈值

默认情况下，当受监视目录的可用空间少于总可用空间的 10% 时，SUSE Manager 会创建警告。当受监视目录的可用空间低于总可用空间的 5% 时，将创建关键警报。

您可以使用 `spacecheck_free_alert` 和 `spacecheck_free_critical` 参数更改这些警报阈值。

例如：

```
spacecheck_free_alert = 10
spacecheck_free_critical = 5
```

9.3. 关闭服务

默认情况下，当达到关键警报阈值时，SUSE Manager 会关闭 spacewalk 服务。

您可以使用 `spacecheck_shutdown` 参数更改此行为。`true` 值启用关闭功能。任何其他值禁用关闭功能。

例如：

```
spacecheck_shutdown = true
```

9.4. 禁用空间检查

默认已启用空间检查工具。您可以使用以下命令完全禁用此工具：

```
systemctl stop spacewalk-diskcheck.timer
systemctl disable spacewalk-diskcheck.timer
```

禁用 `spacewalk-diskcheck.timer` 后，如果达到警报阈值，将停止发送定期电子邮件警报，但警告通知仍会显示在登录页面的顶部。

Chapter 10. 映像构建和管理

10.1. 映像构建概述

SUSE Manager 允许系统管理员构建容器和操作系统映像，并将结果推送到映像存储区。工作流程如下：

过程：构建和推送映像

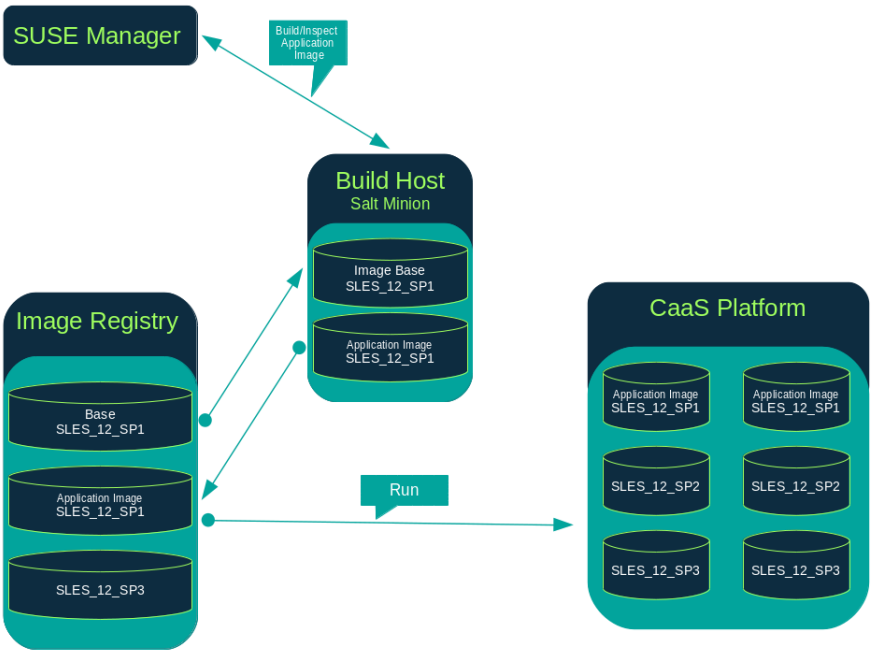
1. 定义映像存储区
2. 定义一个映像配置文件并将其与源（git 储存库或目录）相关联
3. 构建映像
4. 将映像推送到映像存储区

SUSE Manager 支持两种不同的构建类型：Dockerfile 和 Kiwi 映像系统。

Kiwi 构建类型用于构建系统映像、虚拟映像和其他映像。Kiwi 构建类型的映像存储区预定义为文件系统目录，其路径为服务器上的 `/srv/www/os-images`。SUSE Manager 通过 HTTPS 从 `//<服务器-FQDN>/os-images/` 提供映像存储区。映像存储区位置是唯一的，不可自定义。

映像存储在 `/srv/www/os-image/ORGANIZATION-ID` 中。

10.2. 容器映像



10.2.1. 要求

容器功能适用于运行 SUSE Linux Enterprise Server 12 或更高版本的 Salt 客户端。在开始之前，请确保您的环境满足以下要求：

- 一个包含 Dockerfile 和配置脚本的已发布 git 储存库。该储存库可以是公用或专用的，应托管在 GitHub、GitLab 或 BitBucket 上。
- 一个正确配置的映像存储区，例如 Docker 注册表。

  有关容器的详细信息，请参见 https://documentation.suse.com/container/all/html/Container-guide/。

10.2.2. 创建构建主机

要使用 SUSE Manager 构建映像，您需要创建并配置一个构建主机。容器构建主机是运行 SUSE Linux Enterprise 12 或更高版本的 Salt 客户端。本节将指导您完成构建主机的初始配置。

> 构建主机上的操作系统必须与目标映像上的操作系统匹配。
>
> 例如，在运行 SUSE Linux Enterprise Server 15（SP2 或更高版本）操作系统版本的构建主机上构建基于 SUSE Linux Enterprise Server 15 的映像。在运行 SUSE Linux Enterprise Server 12 SP5 或 SUSE Linux Enterprise Server 12 SP4 操作系统版本的构建主机上构建基于 SUSE Linux Enterprise Server 12 的映像。
>
> 不支持跨体系结构构建。

在 SUSE Manager Web UI 中，执行以下步骤以配置构建主机：

过程：构建主机

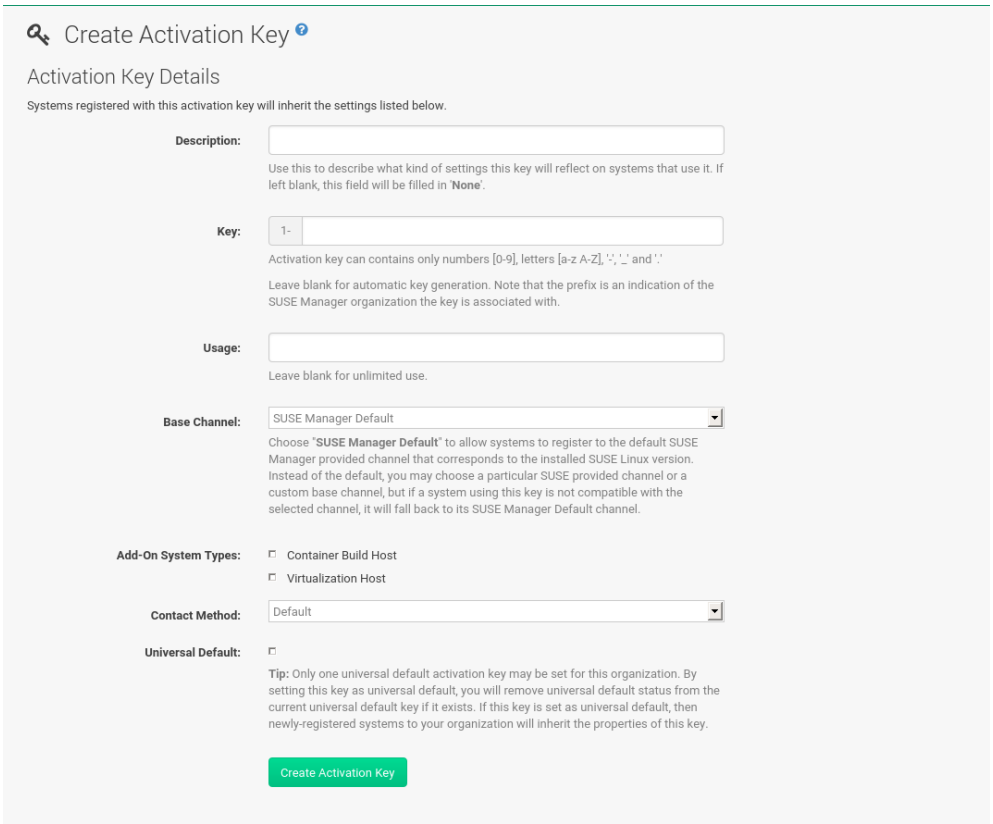
1. 在**系统 › 概览**页面中选择要指定为构建主机的 Salt 客户端。
2. 在所选客户端的系统细节页面中指派容器模块。转到**软件 › 软件通道**并启用容器模块（例如 `SLE-Module-Containers15-Pool` 和 `SLE-Module-Containers15-Updates`）。单击 **[更改订阅]** 以确认。
3. 在**系统细节 › 属性**页面中，从附加系统类型列表中启用容器构建主机，然后单击 **[更新属性]** 以确认。
4. 通过应用 `Highstate` 安装所有必需的软件包。在系统细节页面中选择**状态 › Highstate**，然后单击应用 `Highstate`。或者，从 SUSE Manager Server 命令行应用 Highstate：

   ```
   salt '$your_client' state.highstate
   ```

10.2.3. 为容器创建激活密钥

使用 SUSE Manager 构建的容器使用在构建映像时作为储存库关联到激活密钥的通道。本节将指导您为此目的创建一个临时激活密钥。

要构建容器，需要一个与通道关联的激活密钥，但该通道不能是 `SUSE Manager Default`。



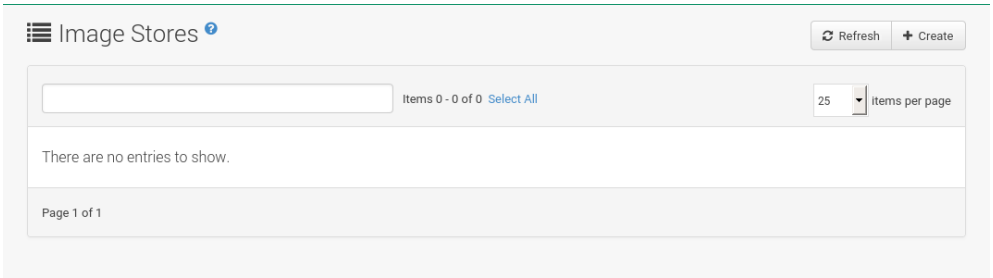
过程：创建激活密钥

1. 选择**系统 › 激活密钥**。
2. 单击 **[创建密钥]**。
3. 输入说明和密钥名称。使用下拉菜单选择要与此密钥关联的基础通道。
4. 单击 **[创建激活密钥]** 确认。

有关详细信息，请参见 **Client-configuration › Activation-keys**。

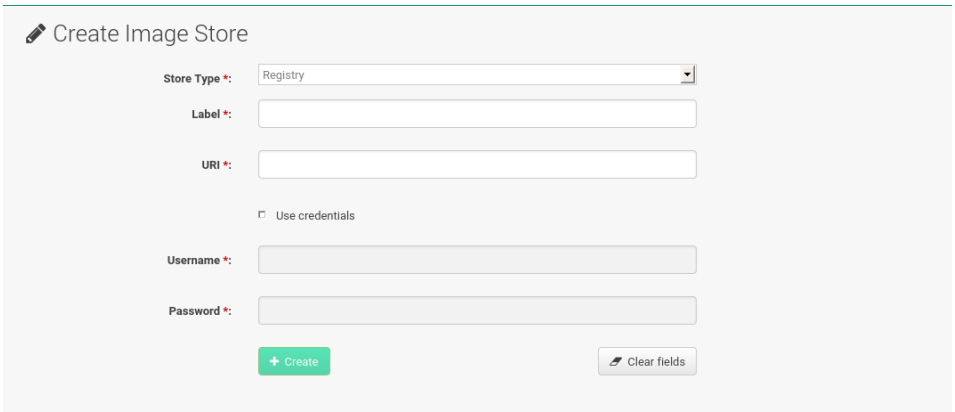
10.2.4. 创建映像存储区

构建的所有映像将推送到映像存储区。本节包含有关创建映像存储区的信息。



过程：创建映像存储区

1. 选择**映像 › 存储区**。
2. 单击创建以创建新存储。



3. 在标签字段中定义映像存储区的名称。
4. 通过填写 `URI` 字段提供映像注册表的路径，该路径用作容器注册表主机（无论是内部还是外部）的完全限定域名 (FQDN)。

```
registry.example.com
```

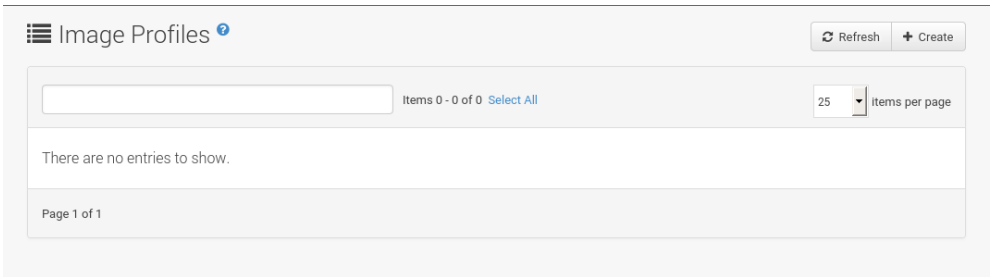
5. 注册表 URI 还可用于指定已被使用的注册表中的映像存储区。

```
registry.example.com:5000/myregistry/myproject
```

6. 单击 **[创建]** 以添加新的映像存储区。

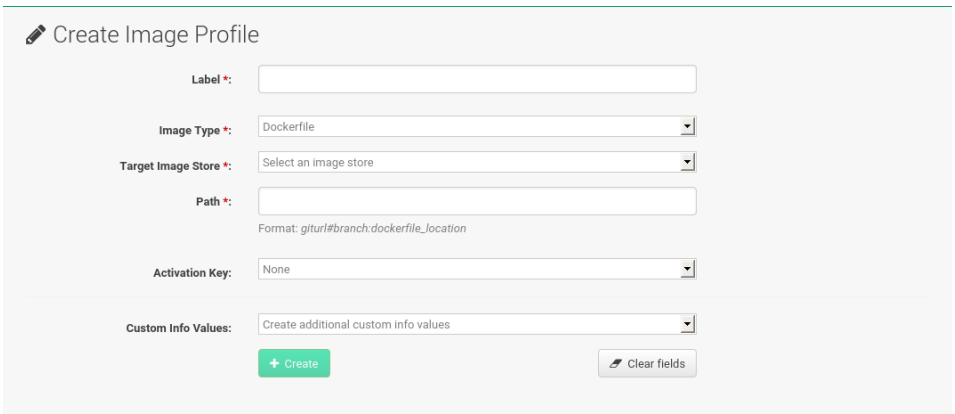
10.2.5. 创建映像配置文件

所有容器映像都是使用包含构建说明的映像配置文件构建的。本节包含有关使用 SUSE Manager Web UI 创建映像配置文件的信息。



过程：创建映像配置文件

1. 要创建映像配置文件，请选择**映像 › 配置文件**，然后单击 **[创建]**。



2. 通过填写标签字段提供映像配置文件的名称。

> 如果您的容器映像标记采用类似于 `myproject/myimage` 的格式，请确保您的映像存储区注册表 URI 包含 `/myproject` 后缀。

3. 使用 Dockerfile 作为映像类型。
4. 使用下拉菜单从目标映像存储区字段中选择您的注册表。
5. 在路径字段中，键入 GitHub、GitLab 或 BitBucket 储存库 URL。该 URL 应该是 http、https 或令牌身份验证 URL。使用以下格式之一：

GitHub 路径选项

- GitHub 单用户项目储存库

  https://github.com/USER/project.git#branchname:folder

- GitHub 组织项目储存库

  https://github.com/ORG/project.git#branchname:folder

- GitHub 令牌身份验证

  如果您的 git 储存库是专用的，请修改配置文件的 URL 以包含身份验证。使用以下 URL 格式通过 GitHub 令牌进行身份验证：

  https://USER:<身份验证令牌>@github.com/USER/project.git#master:/container/

- GitLab 单用户项目储存库

  https://gitlab.example.com/USER/project.git#master:/container/

- GitLab 组项目储存库

  https://gitlab.example.com/GROUP/project.git#master:/container/

- GitLab 令牌身份验证

  如果您的 git 储存库是专用的且不可公开访问，则需要修改配置文件的 git URL 以包含身份验证。使用以下 URL 格式通过 GitLab 令牌进行身份验证：

  https://gitlab-ci-token:<身份验证令牌>@gitlab.example.com/USER/project.git#master:/container/

  > 如果您未指定 git 分支，则默认会使用 `master` 分支。如果未指定 `folder`，则映像源（Dockerfile 源）预期位于 GitHub 或 GitLab checkout 分支的根目录中。

6. 选择一个激活密钥。激活密钥可确保将使用配置文件的映像指派到正确的通道和软件包。

   > 将激活密钥与映像配置文件关联后，可以确保使用该配置文件的任何映像都会使用正确的软件通道以及该通道中的任何软件包。

7. 单击 **[创建]** 按钮。

示例 Dockerfile 源

https://github.com/SUSE/manager-build-profiles 上发布了可重复使用的映像配置文件

> `ARG` 参数确保构建的映像与 SUSE Manager 提供的所需储存库相关联。`ARG` 参数还可用于构建不同于构建主机本身所用 SUSE Linux Enterprise Server 版本的 SUSE Linux Enterprise Server 映像版本。
>
> 例如：`ARG repo` 参数以及指向储存库文件的 `echo` 命令创建正确的路径，然后将其注入到所需通道版本的储存库文件中。
>
> 储存库由您指派到映像配置文件的激活密钥决定。

```
FROM registry.example.com/sles12sp2
MAINTAINER Tux Administrator "tux@example.com"

### 开始：这些行需要与 {productname} 配合使用

ARG repo
ARG cert

# 添加正确的证书
RUN echo "$cert" > /etc/pki/trust/anchors/RHN-ORG-TRUSTED-SSL-CERT.pem

# 更新证书信任存储
RUN update-ca-certificates

# 将储存库路径添加到映像
RUN echo "$repo" > /etc/zypp/repos.d/susemanager:dockerbuild.repo

### 结束：这些行需要与 {productname} 配合使用

# 添加打包脚本
ADD add_packages.sh /root/add_packages.sh

# 运行打包脚本
RUN /root/add_packages.sh

# 构建后从映像中去除储存库路径
RUN rm -f /etc/zypp/repos.d/susemanager:dockerbuild.repo
```

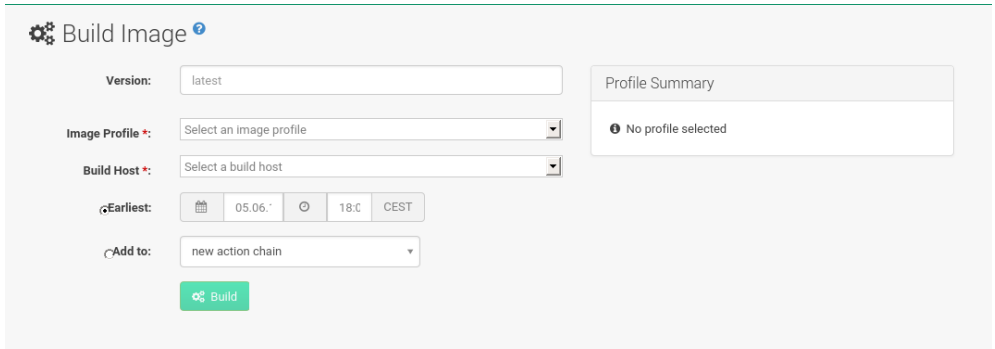
10.2.5.1. 使用自定义信息键-值对作为 Docker `buildargs`

您可以指派自定义信息键-值对，以将信息挂接到映像配置文件。此外，这些键-值对将作为 `buildargs` 传递给 Docker 构建命令。

有关可用自定义信息键和创建其他信息键的详细信息，请参见 **Reference › Systems**。

10.2.6. 构建映像

可通过两种方式构建映像。可以在左侧导航栏中选择**映像 › 构建**，或单击**映像 › 配置文件**列表中的构建图标。



过程：构建映像

1. 选择**映像 › 构建**。
2. 如果您不想使用默认的最新版本（仅与容器相关），而要使用其他版本，请添加不同的标记名称。
3. 选择构建配置文件和构建主机。

> 请注意构建字段右侧的配置文件摘要。在您选择构建配置文件后，有关所选配置文件的详细信息将显示在此区域中。

4. 要安排构建，请单击 **[构建]** 按钮。

10.2.7. 导入映像

您可以导入和检查任意映像。在左侧导航栏中选择**映像 › 映像列表**。填写导入对话框的文本框。处理完成后，导入的映像将列在映像列表页面上。

过程：导入映像

1. 在**映像 › 映像列表**中，单击 **[导入]** 打开导入映像对话框。
2. 在导入映像对话框中填写以下字段：

   映像存储区

   要从中拉取映像进行检查的注册表。

   映像名称

   注册表中映像的名称。

   映像版本

   注册表中映像的版本。

   构建主机

   用于拉取和检查映像的构建主机。

   激活密钥

   激活密钥，它提供用于检查映像的软件通道的路径。

3. 单击 **[导入]** 以确认。

随即会在数据库中创建映像项，并在 SUSE Manager 上安排检查映像操作。

处理完成后，您可以在映像列表中找到已导入的映像。它在构建列中显示了一个不同的图标，指示该映像已导入。也可以在映像的概览选项卡上看到已导入映像的状态图标。

10.2.8. 查错

下面是处理映像时存在的一些已知问题：

- 用于访问注册表或 git 储存库的 HTTPS 证书应通过自定义状态文件部署到客户端。
- 目前不支持使用 Docker 进行 SSH git 访问。

10.3. 操作系统映像

操作系统映像由 Kiwi 映像系统构建。输出映像可自定义，可以是 PXE、QCOW2、LiveCD 或其他类型的映像。

有关 Kiwi 构建系统的详细信息，请参见 Kiwi 文档。

10.3.1. 要求

Kiwi 映像构建功能适用于运行 SUSE Linux Enterprise Server 12 和 SUSE Linux Enterprise Server 11 的 Salt 客户端。

必须可在以下位置之一访问 Kiwi 映像配置文件和配置脚本：

- Git 储存库
- HTTP 托管 tarball
- 本地构建主机目录

有关 git 提供的完整 Kiwi 储存库的示例，请参见 https://github.com/SUSE/manager-build-profiles/tree/master/OSImage。

对于运行使用 Kiwi 构建的操作系统映像的主机，至少需要提供 1 GB RAM。具体所需磁盘空间取决于映像的实际大小。有关详细信息，请参见底层系统的文档。

构建主机必须是 Salt 客户端。不要将构建主机安装为传统客户端。

10.3.2. 创建构建主机

要使用 SUSE Manager 构建各种映像，请创建并配置一个构建主机。操作系统映像构建主机是在 SUSE Linux Enterprise Server 15（SP2 或更高版本）或SUSE Linux Enterprise Server 12（SP4 或更高版本）上运行的 Salt 客户端。

此过程将指导您完成构建主机的初始配置。

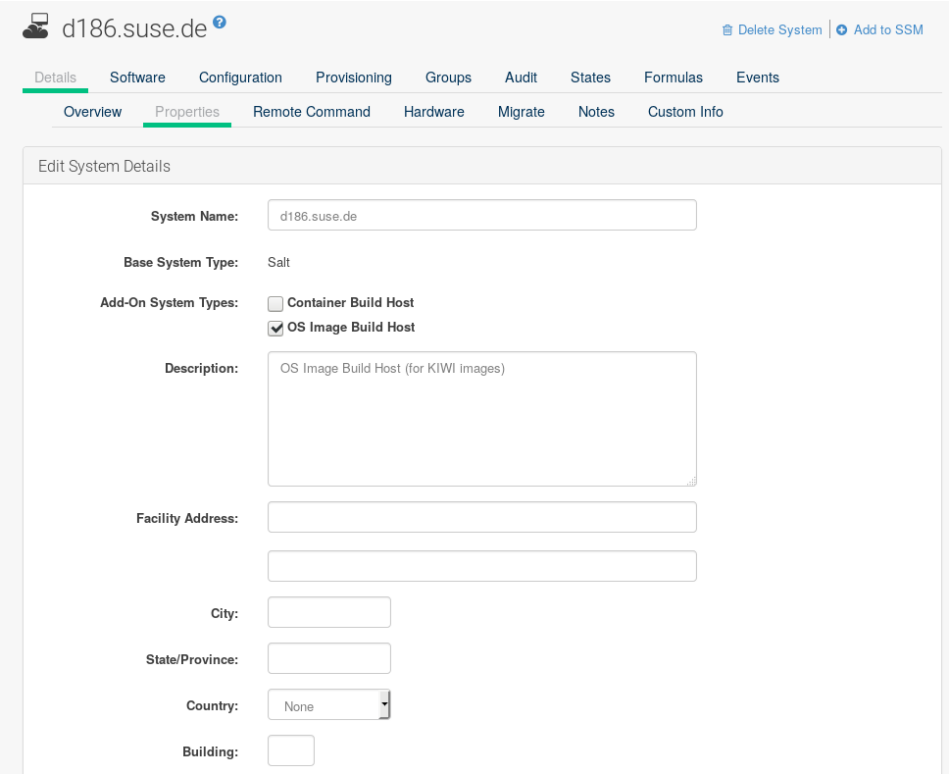
构建主机上的操作系统必须与目标映像上的操作系统匹配。

例如，在运行 SUSE Linux Enterprise Server 15（SP2 或更高版本）操作系统版本的构建主机上构建基于 SUSE Linux Enterprise Server 15 的映像。在运行 SUSE Linux Enterprise Server 12 SP5 或 SUSE Linux Enterprise Server 12 SP4 操作系统版本的构建主机上构建基于 SUSE Linux Enterprise Server 12 的映像。

无法实现跨体系结构的构建。例如，必须在运行 SUSE Linux Enterprise Server 15 SP3 的 Raspberry PI（aarch64 体系结构）构建主机上构建 Raspberry PI SUSE Linux Enterprise Server 15 SP3 映像。

过程：在 SUSE Manager Web UI 中配置构建主机

1. 在**系统 › 概览**页面中选择要指定为构建主机的客户端。
2. 导航到**系统细节 › 属性**选项卡，为附加系统类型启用操作系统映像构建主机。单击 **[更新属性]** 确认。



3. 导航到**系统细节 › 软件 › 软件通道**，根据构建主机版本启用所需的软件通道。
   - SUSE Linux Enterprise Server 12 构建主机需要 SUSE Manager 客户端工具（`SLE-Manager-Tools12-Pool` 和 `SLE-Manager-Tools12-Updates`）。
   - SUSE Linux Enterprise Server 15 构建主机需要 SUSE Linux Enterprise Server 模块 `SLE-Module-DevTools15-SP4-Pool` 和 `SLE-Module-DevTools15-SP4-Updates`。配置日程安排，然后单击 **[确认]**。
4. 通过应用 `Highstate` 安装 Kiwi 和所有必需的软件包。在系统细节页面中选择**状态 › Highstate**，然后单击 **[应用 Highstate]**。或者，从 SUSE Manager Server 命令行应用 Highstate：

```
salt '$your_client' state.highstate
```

10.3.2.1. SUSE Manager Web 服务器公共证书 RPM

构建主机置备将 SUSE Manager 证书 RPM 复制到构建主机。此证书用于访问 SUSE Manager 提供的储存库。

该证书由 `mgr-package-rpm-certificate-osimage` 打包脚本打包在 RPM 中。在全新安装 SUSE Manager 期间会自动调用该打包脚本。

当您升级 `spacewalk-certs-tools` 软件包时，升级方案会使用默认值调用该打包脚本。但是，如果证书路径已更改或不可用，请在升级过程完成后使用 `--ca-cert-full-path <证书路径>` 手动调用该打包脚本。

10.3.2.2. 打包脚本调用示例

```
/usr/sbin/mgr-package-rpm-certificate-osimage --ca-cert-full-path /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
```

包含证书的 RPM 软件包存储在 Salt 可访问的目录中，例如：

```
/usr/share/susemanager/salt/images/rhn-org-trusted-ssl-cert-osimage-1.0-1.noarch.rpm
```

包含证书的 RPM 软件包在本地构建主机储存库中提供：

```
/var/lib/Kiwi/repo
```

在构建源中指定包含 SUSE Manager SSL 证书的 RPM 软件包，并确保您的 Kiwi 配置包含 `rhn-org-trusted-ssl-cert-osimage` 作为 `bootstrap` 部分中必需的软件包。

列表 4. config.xml

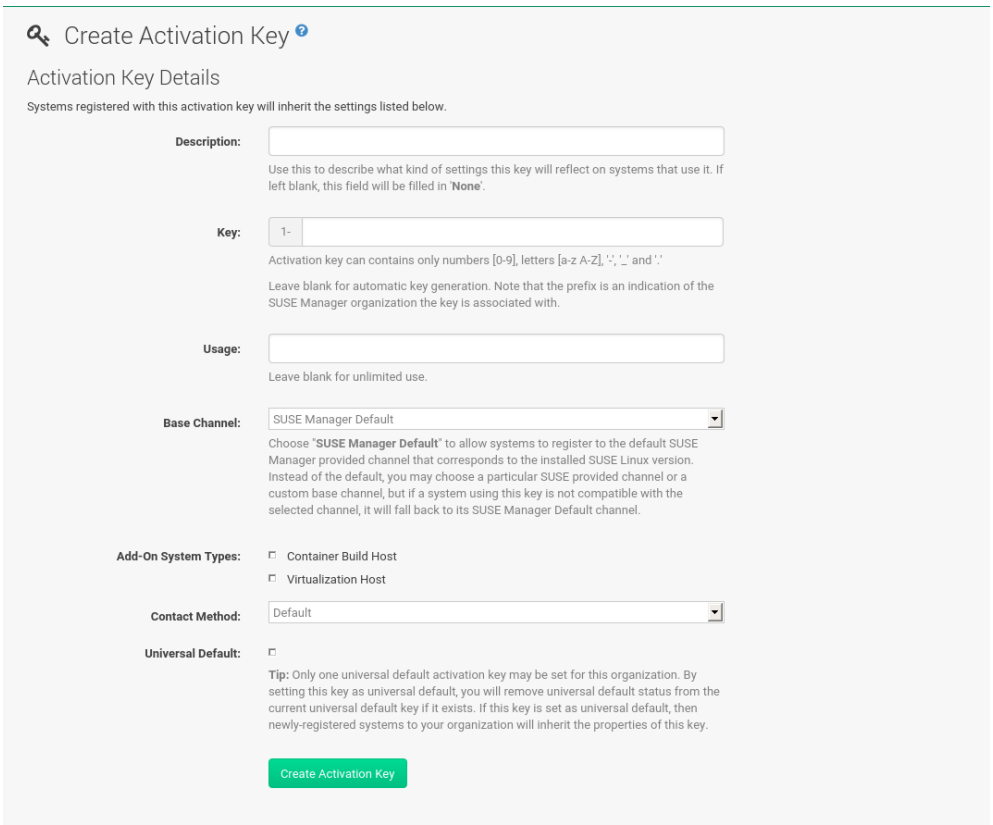
```
...
 <packages type="bootstrap">
  ...
  <package name="rhn-org-trusted-ssl-cert-osimage" bootinclude="true"/>
 </packages>
...
```

10.3.3. 为操作系统映像创建激活密钥

创建与通道（在构建映像时操作系统映像可将其用作储存库）关联的激活密钥。

必须提供激活密钥才能构建操作系统映像。

要构建操作系统映像，需要一个与通道关联的激活密钥，但该通道不能是 `SUSE Manager Default`。



过程：创建激活密钥

1. 在 Web UI 中，选择**系统 › 激活密钥**。
2. 单击创建密钥。
3. 输入说明和密钥名称，并使用下拉框选择要与该密钥关联的基础通道。
4. 单击 **[创建激活密钥]** 确认。

有关详细信息，请参见 **Client-configuration › Activation-keys**。

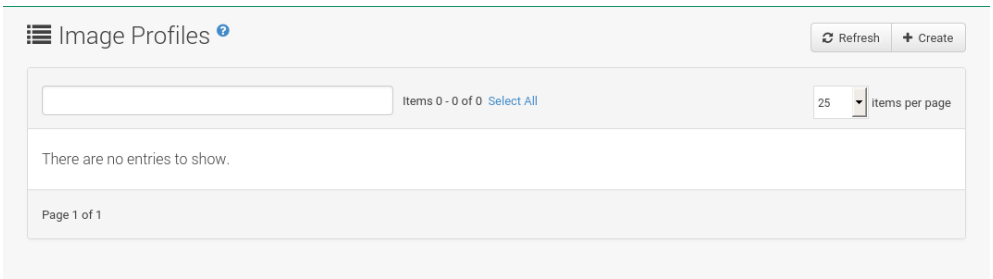
10.3.4. 创建映像存储区

操作系统映像可能需要大量存储空间。因此，我们建议将操作系统映像存储区放在其自身所在的分区上或 Btrfs 子卷上，并与根分区分开。默认情况下，映像存储区位于 `/srv/www/os-images`。

> 目前不支持 Kiwi 构建类型的用于构建系统映像、虚拟映像和其他映像的映像存储区。
>
> 映像始终存储在 `/srv/www/os-images/<组织-ID>` 中，可通过 HTTP/HTTPS https://<susemanager_主机>/os-images/<组织 ID> 访问。

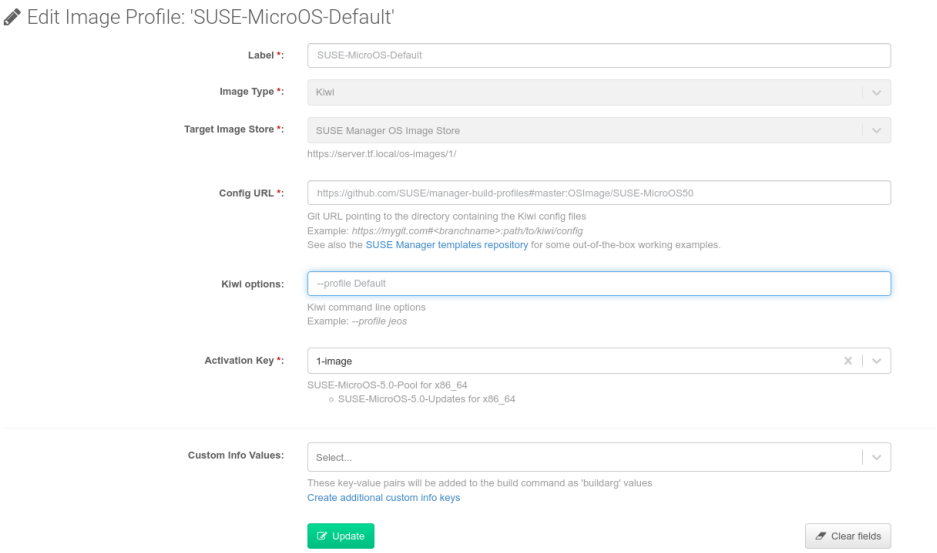
10.3.5. 创建映像配置文件

使用 Web UI 管理映像配置文件。



过程：创建映像配置文件

1. 要创建映像配置文件，请在**映像 › 配置文件**中选择，然后单击 [**创建**]。



2. 在标签字段中，提供映像配置文件的名称。
3. 使用 `Kiwi` 作为映像类型。
4. 系统会自动选择映像存储区。
5. 输入指向包含 Kiwi 配置文件的目录的配置 `URL`：
   a. git URI
   b. HTTPS tarball
   c. 构建主机本地目录的路径
6. 根据需要输入 `Kiwi 选项`。如果 Kiwi 配置文件指定了多个配置文件，请使用 `--profile <名称>` 选择活动配置文件。 有关其他选项，请参见 Kiwi 文档。
7. 选择一个激活密钥。激活密钥可确保将使用配置文件的映像指派到正确的通道和软件包。

> 将激活密钥与映像配置文件相关联，以确保映像配置文件使用正确的软件通道和任何软件包。

8. 单击 [**创建**] 按钮确认。

源格式选项

- 指向储存库的 git/HTTP(S) URL

  指向要构建的映像的源所在 git 储存库的 URL。根据储存库的布局，该 URL 可能是：

  https://github.com/SUSE/manager-build-profiles

  可以在 URL 中的 `#` 字符后面指定一个分支。此示例使用了 `master` 分支：

  https://github.com/SUSE/manager-build-profiles#master

  可以在 `:` 字符后面指定包含映像源的目录。此示例使用了 `OSImage/POS_Image-JeOS6`：

  https://github.com/SUSE/manager-build-profiles#master:OSImage/POS_Image-JeOS6

- 指向 tarball 的 HTTP(S) URL

  指向托管在 Web 服务器上的 tar 存档（压缩或未压缩）的 URL。

  https://myimagesourceserver.example.org/MyKiwiImage.tar.gz

- 构建主机上的目录的路径

  输入包含 Kiwi 构建系统源的目录的路径。此目录必须在选定的构建主机上存在。

  /var/lib/Kiwi/MyKiwiImage

10.3.5.1. Kiwi 源的示例

Kiwi 源至少包含 `config.xml`。通常其中还有 `config.sh` 和 `images.sh`。源还可以包含要安装在 `root` 子目录下的最终映像中的文件。

有关 Kiwi 构建系统的信息，请参见 Kiwi 文档。

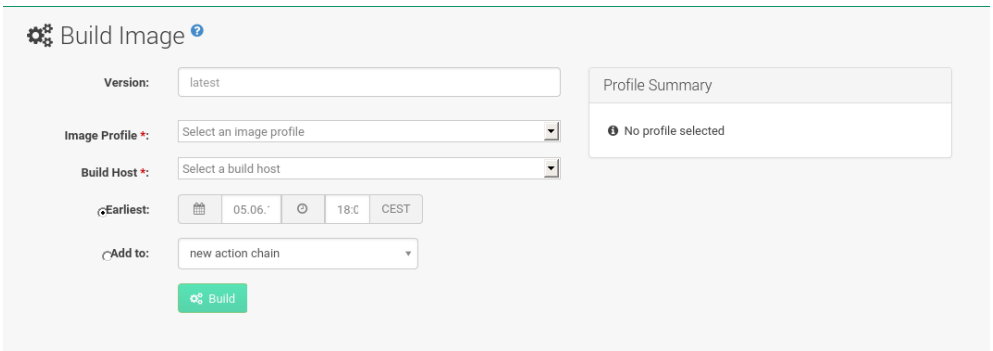
SUSE 在 SUSE/manager-build-profiles 公共 GitHub 储存库中提供了功能齐备的映像源的示例。

列表 5. JeOS config.xml 示例

```
<?xml version="1.0" encoding="utf-8"?>

<image schemaversion="6.1" name="POS_Image_JeOS6">
  <description type="system">
    <author>Admin User</author>
    <contact>noemail@example.com</contact>
    <specification>SUSE Linux Enterprise 12 SP3 JeOS</specification>
  </description>
  <preferences>
    <version>6.0.0</version>
    <packagemanager>zypper</packagemanager>
    <bootsplash-theme>SLE</bootsplash-theme>
    <bootloader-theme>SLE</bootloader-theme>

    <locale>en_US</locale>
    <keytable>us.map.gz</keytable>
    <timezone>Europe/Berlin</timezone>
    <hwclock>utc</hwclock>

    <rpm-excludedocs>true</rpm-excludedocs>
    <type boot="saltboot/suse-SLES12" bootloader="grub2" checkprebuilt="true" compressed
="false" filesystem="ext3" fsmountoptions="acl" fsnocheck="true" image="pxe" kernelcmdline
="quiet"></type>
  </preferences>
  <!--   CUSTOM REPOSITORY
  <repository type="rpm-dir">
   <source path="this://repo"/>
  </repository>
  -->
  <packages type="image">
    <package name="patterns-sles-Minimal"/>
    <package name="aaa_base-extras"/> <!-- wouldn't be SUSE without that ;-) -->
    <package name="kernel-default"/>
    <package name="salt-minion"/>
    ...
  </packages>
  <packages type="bootstrap">
    ...
    <package name="sles-release"/>
    <!-- this certificate package is required to access {productname} repositories
       and is provided by {productname} automatically -->
    <package name="rhn-org-trusted-ssl-cert-osimage" bootinclude="true"/>

  </packages>
  <packages type="delete">
    <package name="mtools"/>
    <package name="initviocons"/>
    ...
  </packages>
</image>
```

10.3.6. 构建映像

可以使用 Web UI 以两种方式构建映像。选择**映像 › 构建**，或单击**映像 › 配置文件**列表中的构建图标。



过程：构建映像

1. 选择**映像 › 构建**。
2. 如果您不想使用默认的最新版本（仅适用于容器），而要使用其他版本，请添加不同的标记名称。
3. 选择映像配置文件和构建主机。

> 构建字段右侧会显示配置文件摘要。在您选择构建配置文件后，有关所选配置文件的详细信息将显示在此处。

4. 要安排构建，请单击 **[构建]** 按钮。

> 在映像构建过程中，构建服务器无法运行任何形式的自动挂载程序。如果适用，请确保不要以 root 身份运行 Gnome 会话。如果某个自动挂载程序正在运行，则映像构建可以成功完成，但映像的校验和将会不同，从而导致失败。

成功构建映像后，检查阶段随即开始。在检查阶段，SUSE Manager 会收集有关映像的信息：

- 映像中安装的软件包列表
- 映像的校验和
- 映像类型和其他映像细节

> 如果构建的映像类型是 PXE，则还会生成一个 Salt pillar。映像 pillar 存储在数据库中，Salt 子系统可以访问有关生成的映像的细节。细节包括映像文件所在位置和提供映像文件的位置、映像校验和、网络引导所需的信息，等等。
>
> 生成的 pillar 可供所有连接的客户端使用。

10.3.7. 查错

构建映像需要完成几个相关的步骤。如果构建失败，调查 Salt 状态结果和构建日志可能有助于确定失败原因。构建失败时，可以执行以下检查：

- 构建主机是否可以访问构建源
- 构建主机和 SUSE Manager 服务器上是否为映像提供了足够的磁盘空间

- 激活密钥是否关联了正确的通道
- 使用的构建源是否有效
- 包含 SUSE Manager 公共证书的 RPM 软件包是否是最新的，并已在路径 `/usr/share/susemanager/salt/images/rhn-org-trusted-ssl-cert-osimage-1.0-1.noarch.rpm` 下提供。有关如何刷新公共证书 RPM 的详细信息，请参见 创建构建主机。

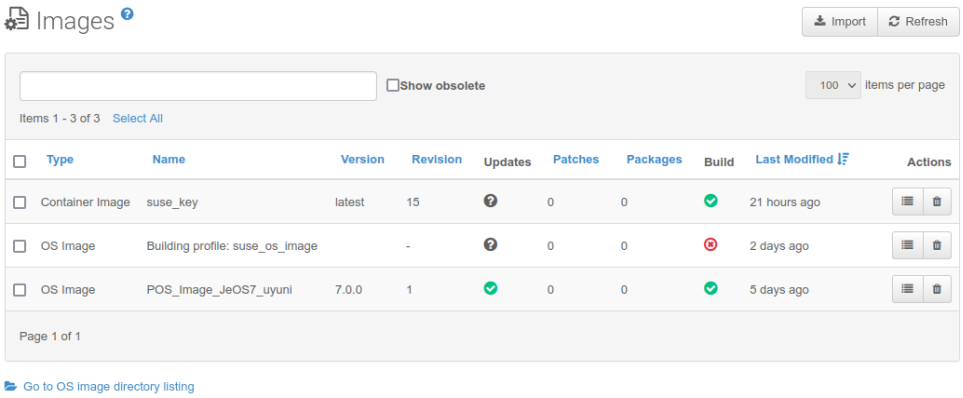
10.3.8. 限制

本节包含使用映像时存在的一些已知问题。

- 用于访问 HTTP 源或 git 储存库的 HTTPS 证书应通过自定义状态文件部署到客户端，或手动进行配置。
- 不支持导入基于 Kiwi 的映像。

10.4. 构建的映像列表

要列出可用的已构建映像，请选择**映像 › 映像列表**。此时会显示所有映像的列表。



显示的映像相关数据包括映像的名称、版本、修订版和构建状态。还可以查看映像更新状态，以及可能适用于该映像的补丁和软件包更新列表。

对于操作系统映像，名称和版本字段值源自 Kiwi 源，在成功完成构建后会更新。在构建期间或构建失败后，这些字段会根据配置文件名称显示一个临时名称。

修订版会在每次成功构建后自动递增。对于操作系统映像，多个修订版可以在存储中共存。

对于容器映像，存储中只会保存最新版本。有关旧修订版（软件包、补丁等）的信息将会保留，可以使用显示过时项复选框列出这些修订版。

单击映像上的 **[细节]** 按钮会显示一个详细视图。详细视图包含相关补丁的确切列表、映像中安装的所有软件包的列表和构建日志。

单击 **[删除]** 按钮会从列表中删除映像。同时还会删除操作系统映像存储区中关联的 pillar 和文件，以及过时的修订版。

仅当构建后的检查状态为成功时，才会显示补丁和软件包列表。

Chapter 11. 基础结构维护任务

如果您使用安排的停机时段，可能发现很难记住在 SUSE Manager Server 发生这种事关重大的停机之前、期间和之后您要做的所有事情。SUSE Manager Server 相关系统（例如服务器间同步从属服务器或 SUSE Manager Proxy）也会受到影响，必须在日程安排中将其考虑在内。

SUSE 建议您始终将 SUSE Manager 基础结构保持在最新状态。其中包括服务器、代理和构建主机。 如果您不将 SUSE Manager 服务器保持在最新状态，则可能在需要更新环境中的某些组件时，将无法成功更新。

本章提供了一份停机时段核对清单，其中包含有关执行每个步骤的更多信息的链接。

11.1. 服务器

1. 应用最新更新。 请参见 **Installation-and-upgrade › Server-intro**。
2. 根据需要升级到最新服务包。
3. 运行 `spacewalk-service status` 并检查所有必需的服务是否已正常运行。

有关数据库纲要升级和 PostgreSQL 迁移的信息，请参见 **Installation-and-upgrade › Db-intro**。

您可以使用软件包管理器安装更新。

- 有关使用 YaST 的详细信息，请参见 https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-onlineupdate-you.html。
- 有关使用 zypper 的详细信息，请参见 https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-sw-cl.html#sec-zypper。

默认会为 SUSE Manager Server 配置并启用多个更新通道。新软件包和更新的软件包会自动变为可用状态。

要使 SUSE Manager 保持最新，请将其直接连接到 SUSE Customer Center 或使用Repository Management Tool (RMT)。可以将 RMT 用作断开连接的环境的本地安装源。

可以使用以下命令检查更新通道是否在您的系统上可用：

```
zypper lr
```

输出如下所示：

```
Name                                                    | Enabled | GPG Check | Refresh
--------------------------------------------------------+---------+-----------+--------
SLE-Module-Basesystem15-SP2-Pool                        | Yes     | (r ) Yes  | No
SLE-Module-Basesystem15-SP2-Updates                     | Yes     | (r ) Yes  | Yes
SLE-Module-Python2-15-SP2-Pool                          | Yes     | (r ) Yes  | No
SLE-Module-Python2-15-SP2-Updates                       | Yes     | (r ) Yes  | Yes
SLE-Product-SUSE-Manager-Server-4.1-Pool                | Yes     | (r ) Yes  | No
SLE-Product-SUSE-Manager-Server-4.1-Updates             | Yes     | (r ) Yes  | Yes
SLE-Module-SUSE-Manager-Server-4.1-Pool                 | Yes     | (r ) Yes  | No
SLE-Module-SUSE-Manager-Server-4.1-Updates              | Yes     | (r ) Yes  | Yes
SLE-Module-Server-Applications15-SP2-Pool               | Yes     | (r ) Yes  | No
SLE-Module-Server-Applications15-SP2-Updates            | Yes     | (r ) Yes  | Yes
SLE-Module-Web-Scripting15-SP2-Pool                     | Yes     | (r ) Yes  | No
SLE-Module-Web-Scripting15-SP2-Updates                  | Yes     | (r ) Yes  | Yes
```

SUSE Manager 会发布维护更新 (MU) 以提供较新的软件包。维护更新用新的版本号表示。例如，在发布 MU 后，主发行版 4.1 将递增为 4.1.1。

可以通过查看 Web UI 中导航栏底部的信息来校验您正在运行的版本。还可以使用 `api.getVersion()` XMLRPC API 调用来获取版本号。

11.1.1. 客户端工具

当服务器更新时，请考虑同时更新客户端上的某些工具。并非一定要更新客户端上的 `salt-minion`、`zypper` 和其他相关管理软件包，但一般情况下最好这样做。例如，服务器上的维护更新可能会引入新的 Salt 主版本。然后，Salt 客户端有一段时间可以继续正常运行，但后来可能会出现问题。为了避免这种情况，在适当的情况下请务必更新 `salt-minion` 软件包。SUSE 确保始终可以安全更新 `salt-minion`。

11.2. 服务器间同步从属服务器

如果您使用服务器间同步从属服务器，请在 SUSE Manager Server 更新完成后对其进行更新。

有关服务器间同步的详细信息，请参见 **Administration › Iss**。

11.3. 监视服务器

如果您使用 Prometheus 监视服务器，请在 SUSE Manager Server 更新完成后对其进行更新。

有关监视的详细信息，请参见 **Administration › Monitoring**。

11.4. 代理

SUSE Manager Server 更新完成后，代理应会立即更新。

一般情况下，不支持运行与其他版本上的服务器相连接的代理。唯一的例外情况是在更新期间，预期首先会更新服务器，因此代理可能暂时运行旧版本。

尤其是从版本 4.0 迁移到版本 4.1 时，请先升级服务器，然后再升级任何代理。

有关详细信息，请参见 **Installation-and-upgrade › Proxy-intro**。

Chapter 12. 服务器间同步

如果您安装了多个 SUSE Manager，有时需要在服务器之间复制内容。使用服务器间同步 (ISS) 可以导出一台服务器（源）的数据，并将其导入另一台（目标）服务器。这对于中心部署方案或断开连接的设置很有用。

> 在第 2 版 ISS 实现中，SUSE 去除了主从概念。可以在任何 SUSE Manager 服务器之间朝任一方向导出和导入内容。

12.1. 服务器间同步 - 版本 1

如果您安装了多个 SUSE Manager，需要确保它们在内容和权限方面保持一致。服务器间同步 (ISS) 允许连接两个或更多个 SUSE Manager Server 并使它们保持最新。

要设置 ISS 版本 1，需要将一个 SUSE Manager 服务器定义为主服务器，将另一个定义为从属服务器。如果配置有冲突，系统会优先使用主服务器配置。

> ISS 主服务器之所以称为主服务器，只因为其上挂接了从属服务器。这意味着，需要首先通过定义其从属服务器来设置 ISS 主服务器。然后通过将 ISS 从属服务器挂接到主服务器来设置从属服务器。

过程：设置 ISS 主服务器

1. 在 SUSE Manager Web UI 中，导航到**管理 › ISS 配置 › 主服务器设置**，然后单击 **[添加新的从属服务器]**。
2. 在编辑从属服务器细节对话框中，为 ISS 主服务器的第一个从属服务器提供以下细节：
   - 在从属服务器的完全限定域名字段中，输入 ISS 从属服务器的 FQDN。 例如：`server2.example.com`。
   - 选中允许从属服务器同步？复选框以启用从属服务器与主服务器的同步。
   - 选中将所有组织同步到从属服务器？复选框以将所有组织同步到此从属服务器。
3. 单击 **[创建]** 以添加 ISS 从属服务器。
4. 在允许导出所选组织部分，选中您要允许在其中将此从属服务器导出到主服务器的组织，然后单击 **[允许组织]**。

在设置 ISS 从属服务器之前，需要确保拥有适当的 CA 证书。

过程：将主服务器 CA 证书复制到 ISS 从属服务器

1. 在 ISS 主服务器上的 `/srv/www/htdocs/pub/RHN-ORG-TRUSTED-SSL-CERT` 中找到 CA 证书，并创建一个可传输到 ISS 从属服务器的副本。
2. 在 ISS 从属服务器上，将 CA 证书文件保存到 `/etc/pki/trust/anchors/` 目录。

复制证书后，可以设置 ISS 从属服务器。

过程：设置 ISS 从属服务器

1. 在 SUSE Manager Web UI 中，导航到**管理 › ISS 配置 › 从属服务器设置**，然后单击 **[添加新的主服务器]**。

2. 在新主服务器细节对话框中，为用作 ISS 主服务器的服务器提供以下细节：
   - 在主服务器的完全限定域名字段中，输入此从属服务器的 ISS 主服务器的 FQDN。 例如：`server1.example.com`。
   - 在此主服务器 CA 证书的文件名字段中，输入 CA 证书在 ISS 主服务器上的绝对路径。 此路径应是 `/etc/pki/trust/anchors/RHN-ORG-TRUSTED-SSL-CERT`。
3. 单击 **[添加新的主服务器]** 将 ISS 从属服务器添加到此主服务器。

过程：完成 ISS 设置

1. 在 ISS 从属服务器上的命令提示符下，与 ISS 主服务器同步：

```
mgr-inter-sync
```

2. 可选：要同步单个通道，请使用以下命令：

```
mgr-inter-sync -c <通道名称>
```

3. 在 SUSE Manager Web UI 中，导航到**管理 › ISS 配置 › 配置主-从属服务器映射**，并选择要同步的组织。

12.2. 服务器间同步 - 版本 2

如果您安装了多个 SUSE Manager，有时需要在服务器之间复制内容。使用服务器间同步 (ISS) 可以导出一台服务器（源）的数据，并将其导入另一台（目标）服务器。这对于中心部署方案或断开连接的设置很有用。

> 在第 2 版 ISS 实现中，SUSE 去除了主从概念。可以在任何 SUSE Manager 服务器之间朝任一方向导出和导入内容。

12.2.1. 安装 ISS 软件包

要使用 ISS，需要在源服务器和目标服务器上安装 `inter-server-sync` 软件包。

12.2.2. 内容同步

过程：导出源服务器上的数据

1. 在源服务器上的命令行中执行 ISS export 命令。`-h` 选项可提供详细帮助：

```
inter-server-sync export -h
```

导出过程会创建一个输出目录，其中包含导入过程所需的所有数据。

过程：将导出目录复制到目标服务器

1. 需要将源服务器中的内容同步到目标服务器。在命令行中，以 root 身份执行以下命令：

```
rsync -r <导出目录的路径> root@<目标服务器>:~/
```

复制所有内容后，开始导入这些内容。

过程：在目标服务器上导入数据

1. 在目标服务器上的命令行中执行 ISS import 命令。`-h` 选项可提供详细帮助：

```
inter-server-sync import -h
```

12.2.3. 数据库连接配置

默认会从 `/etc/rhn/rhn.conf` 加载数据库连接配置。可以使用参数 `--serverConfig` 覆盖属性文件位置。

12.2.4. 已知限制

- 源服务器和目标服务器需使用同一版本。
- 导出和导入组织应该同名。

Chapter 13. SUSE Manager 的在线增补

执行内核更新通常需要重引导系统。应尽早应用公共漏洞和暴露（CVE）补丁，但如果您无法承受停机，可以使用在线增补来注入这些重要更新，这样就不需要重引导。

对于 SLES 12 和 SLES 15，设置在线增补的过程略有不同。本章将阐述适用于这两个版本的过程。

13.1. 设置在线增补通道

每次更新完整的内核软件包后都需要重引导。因此，必须确保使用在线增补的客户端在它们所指派到的通道中没有可用的更新内核。使用在线增补的客户端包含在线增补通道中正在运行的内核的更新。

可通过两种方式管理在线增补通道：

使用内容生命周期管理克隆产品树，并去除比正在运行的版本更新的内核版本。administration:content-lifecycle-examples.pdf 中介绍了此过程。这是建议的解决方法。

或者，可以使用 `spacewalk-manage-channel-lifecycle` 工具。此过程更偏向于手动操作，需要使用命令行工具以及 Web UI。本节针对 SLES 15 SP5 介绍了此过程，但内容同样适用于 SLE 12 SP4 或更高版本。

13.1.1. 为在线增补使用 spacewalk-manage-channel-lifecycle

克隆的供应商通道应该带有前缀 `dev`（表示开发）、`testing` 或 `prod`（表示生产）。在此过程中，您将创建一个 `dev` 克隆通道，然后将该通道升级为 `testing`。

过程：克隆在线增补通道

1. 在客户端上的命令提示符下，以 root 身份获取当前软件包通道树：

```
# spacewalk-manage-channel-lifecycle --list-channels
Spacewalk Username: admin
Spacewalk Password:
Channel tree:

 1. sles15-sp4-pool-x86_64
    \__ sle-live-patching15-pool-x86_64-sp4
    \__ sle-live-patching15-updates-x86_64-sp4
    \__ sle-manager-tools15-pool-x86_64-sp4
    \__ sle-manager-tools15-updates-x86_64-sp4
    \__ sles15-sp4-updates-x86_64
```

2. 结合 `init` 参数使用 `spacewalk-manage-channel` 命令自动创建原始供应商通道的新开发克隆版本：

```
spacewalk-manage-channel-lifecycle --init -c sles15-sp4-pool-x86_64
```

3. 检查通道列表中是否提供了 `dev-sles15-sp4-updates-x86_64`。

检查创建的 `dev` 克隆通道，并去除任何需要重引导的内核更新。

过程：从克隆的通道中去除非在线内核补丁

1. 从**系统 › 系统列表**中选择客户端以检查当前内核版本，并记下内核字段中显示的版本。
2. 在 SUSE Manager Web UI 中，从**系统 › 概述**中选择客户端，导航到**软件 › 管理 › 通道**选项卡，然后选择 `dev-sles15-sp4-updates-x86_64`。 导航到补丁选项卡，然后单击 **[列出/去除补丁]**。
3. 在搜索栏中键入内核，并识别与您的客户端当前使用的内核匹配的内核版本。
4. 去除所有比当前安装的内核更新的内核版本。

现已为您的通道设置了在线增补，可将其升级为 `testing`。在此过程中，您还将随时可应用的在线增补子通道添加到了客户端。

过程：升级在线增补通道

1. 在客户端上的命令提示符下，以 `root` 身份将 `dev-sles15-sp4-pool-x86_64` 通道升级并克隆到新的 `testing` 通道：

```
# spacewalk-manage-channel-lifecycle --promote -c dev-sles15-sp4-pool-x86_64
```

2. 在 SUSE Manager Web UI 中，从**系统 › 概览**中选择客户端，然后导航到**软件 › 软件通道**选项卡。
3. 选中新的 `test-sles15-sp4-pool-x86_64` 自定义通道以更改基础通道，并选中两个相应的在线增补子通道。
4. 单击 **[下一步]**，确认细节正确，然后单击 **[确认]** 以保存更改。

现在可以选择和查看可用的 CVE 补丁，并通过在线增补应用这些重要的内核更新。

13.2. SLES 15 上的在线增补

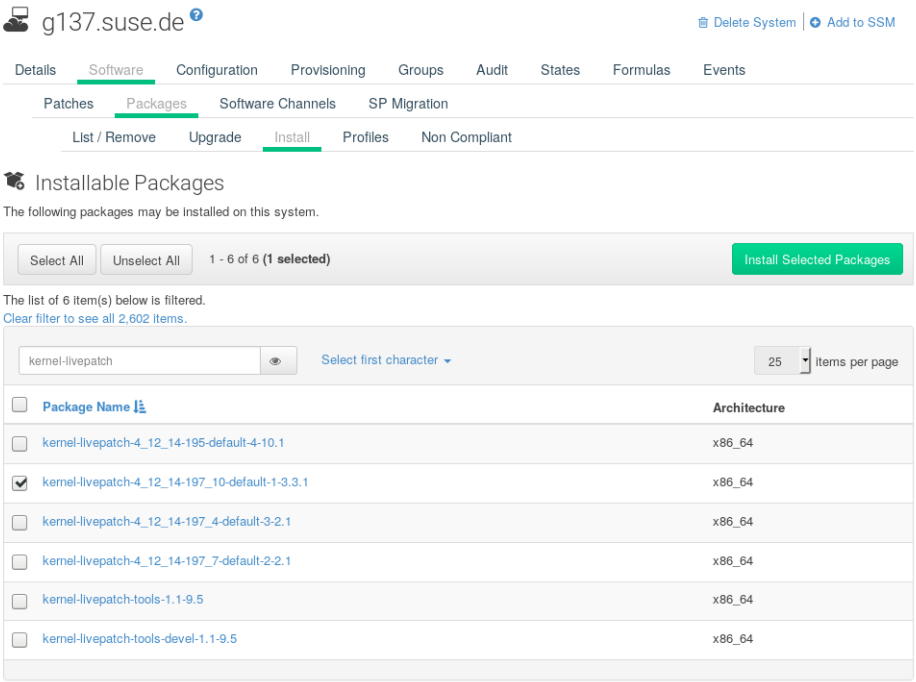
在 SLES 15 和更高版本的系统上，可以通过 `klp livepatch` 工具管理在线增补。

在开始之前，请确保：

- SUSE Manager 已完全更新。
- 您有一个或多个运行 SLES 15（SP1 或更高版本）的 Salt 客户端。
- 您的 SLES 15 Salt 客户端已注册到 SUSE Manager。
- 您有权访问适合您的体系结构的 SLES 15 通道，包括一个或多个在线增补子通道。
- 客户端已完全同步。
- 将客户端指派到为在线增补准备的克隆通道。 有关准备工作的详细信息，请参见 **Administration › Live-patching-channel-setup**。

过程：设置在线增补

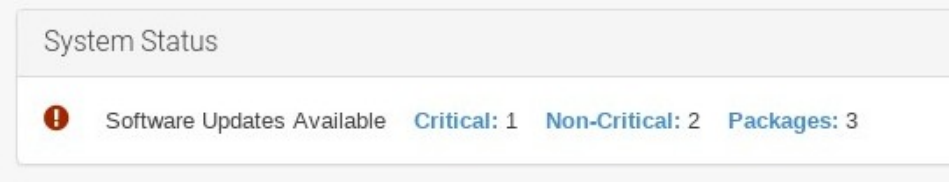
1. 从**系统 › 概览**中选择您要使用在线增补管理的客户端，然后导航到**软件 › 软件包 › 安装**选项卡。 搜索 `kernel-livepatch` 软件包并安装。



2. 应用 Highstate 以启用在线增补，然后重引导客户端。
3. 对您要使用在线增补管理的每个客户端重复上述过程。
4. 要检查是否已正确启用在线增补，请从**系统 › 系统列表**中选择客户端，并确保在线补丁出现在内核字段中。

过程：将在线补丁应用于内核

1. 在 SUSE Manager Web UI 中，从**系统 › 概览**中选择客户端。 屏幕顶部的横幅显示了客户端可用的关键和非关键软件包数量：



2. 单击 **[关键]** 查看可用的关键补丁列表。
3. 选择其摘要显示为重要：`Linux 内核的安全更新`的任何补丁。 安全 bug 还包含其 CVE 编号（如果适用）。
4. 可选：如果您知道要应用的补丁的 CVE 编号，可以在**审计 › CVE 审计**中搜索该补丁，并将它应用于任何需要它的客户端。

- 并非所有内核补丁都是在线补丁。非在线内核补丁由安全盾牌图标旁边的需要重引导图标表示。这些补丁在应用后始终需要重引导。
- 并非所有安全问题都可以通过应用在线补丁来解决。某些安全问题只能通过应用完整内核更新来解决，并需要重引导。针对这些问题指派的 CVE 编号不包含在在线补丁中。CVE 审计会显示此要求。

13.3. SLES 12 上的在线增补

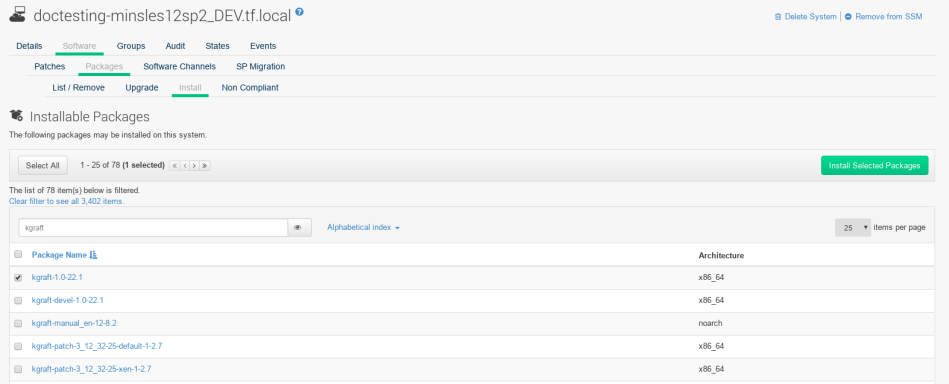
在 SLES 12 系统上，可以通过 kGraft 管理在线增补。有关 kGraft 用法等详细信息，请参见 https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-kgraft.html。

在开始之前，请确保：

- SUSE Manager 已完全更新。
- 您有一个或多个运行 SLES 12（SP1 或更高版本）的 Salt 客户端。
- 您的 SLES 12 Salt 客户端已注册到 SUSE Manager。
- 您有权访问适合您的体系结构的 SLES 12 通道，包括一个或多个在线增补子通道。
- 客户端已完全同步。
- 将客户端指派到为在线增补准备的克隆通道。 有关准备工作的详细信息，请参见 **Administration › Live-patching-channel-setup**。

过程：设置在线增补

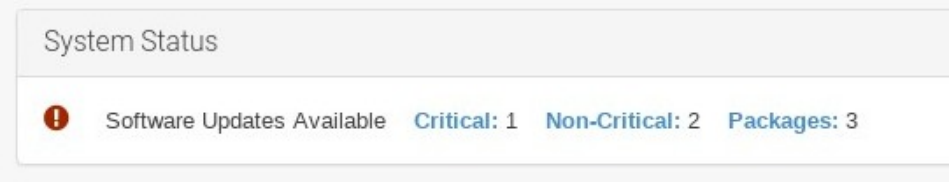
1. 从**系统 › 概览**中选择您要使用在线增补管理的客户端，然后在系统细节页面上导航到**软件 › 软件包 › 安装**选项卡。 搜索 `kgraft` 软件包并安装。



2. 应用 Highstate 以启用在线增补，然后重引导客户端。
3. 对您要使用在线增补管理的每个客户端重复上述过程。
4. 要检查是否已正确启用在线增补，请从**系统 › 系统列表**中选择客户端，并确保在线增补出现在内核字段中。

过程：将在线补丁应用于内核

1. 在 SUSE Manager Web UI 中，从**系统 › 概览**中选择客户端。 屏幕顶部的横幅显示了客户端可用的关键和非关键软件包数量：



2. 单击 **[关键]** 查看可用的关键补丁列表。
3. 选择其摘要显示为重要：`Linux 内核的安全更新`的任何补丁。 安全 bug 还包含其 CVE 编号（如果适用）。
4. 可选：如果您知道要应用的补丁的 CVE 编号，可以在**审计 › CVE 审计**中搜索该补丁，并将它应用于任何需要它的客户端。

- 并非所有内核补丁都是在线补丁。非在线内核补丁由安全盾牌图标旁边的需要重引导图标表示。这些补丁在应用后始终需要重引导。
- 并不是所有安全问题都能通过应用在线补丁来解决。 有些安全问题只能通过应用完整的内核更新来解决，并且此过程需要重引导系统。针对这些问题指派的 CVE 编号不包含在在线补丁中。CVE 审计会显示此要求。

Chapter 14. 维护时段

使用 SUSE Manager 中的维护时段功能，可以将操作安排在预定的维护时段执行。如果您创建了维护时段日程安排并将其应用于客户端，则无法在指定的时段以外执行某些操作。

> 维护时段的工作方式不同于系统锁定。系统锁可按需打开或关闭，而维护时段则是定义允许执行操作的时间段。此外，允许和受限的操作也不相同。有关系统锁的详细信息，请参见 **Client-configuration › System-locking**。

维护时段需要日历和日程安排。日历定义维护时段事件（包括重复性事件）的日期和时间，并且必须采用 `ical` 格式。日程安排使用日历中定义的事件来创建维护时段。必须创建一个要上载的 `ical` 文件，或链接到 `ical` 文件以创建日历，然后才能创建日程安排。

创建日程安排后，可将其指派给已注册到 SUSE Manager Server 的客户端。指派有维护日程安排的客户端在维护时段以外无法运行受限操作。

受限操作会对客户端进行重大修改，可能导致客户端停止运行。受限操作的一些示例包括：

- 软件包安装
- 客户端升级
- 产品迁移
- Highstate 应用（针对 Salt 客户端）

非受限制操作属于次要操作，一般认为它们是安全的，不太可能会在客户端上造成问题。非受限操作的一些示例包括：

- 软件包配置文件更新
- 硬件刷新
- 订阅软件通道

在开始之前，必须创建一个要上载的 `ical` 文件，或链接到 `ical` 文件以创建日历。可以在您偏好的日历工具（例如 Microsoft Outlook、Google Calendar 或 KOrganizer）中创建 `ical` 文件。

过程：上载新的维护日历

1. 在 SUSE Manager Web UI 中，导航到**日程安排 › 维护时段 › 日历**，然后单击 **[创建]**。
2. 在日历名称部分，为日历键入一个名称。
3. 提供 `ical` 文件的 URL，或直接上载该文件。
4. 单击 **[创建日历]** 以保存您的日历。

过程：创建新的日程安排

1. 在 SUSE Manager Web UI 中，导航到**日程安排 › 维护时段 › 日程安排**，然后单击 **[创建]**。
2. 在日程安排名称部分，为日程安排键入一个名称。

3. 可选：如果您的 `ical` 文件包含要应用于多个日程安排的事件，请选中多个。
4. 选择要指派到此日程安排的日历。
5. 单击 **[创建日程安排]** 以保存您的日程安排。

过程：将日程安排指派到客户端

1. 在 SUSE Manager Web UI 中，导航到**系统 › 系统列表**，选择要将日程安排指派到的客户端，找到系统属性面板，然后单击 **[编辑这些属性]**。 或者，可以通过系统集管理器指派客户端，方法是导航到**系统 › 系统集管理器**并使用**其他 › 维护时段**选项卡。
2. 在编辑系统细节页面中，找到维护日程安排字段，然后选择要指派的日程安排的名称。
3. 单击 **[更新属性]** 以指派维护日程安排。

> 当您将新的维护日程安排指派到某个客户端时，可能已经为该客户端安排了一些受限操作，而这些操作现在可能与新的维护日程安排有冲突。如果发生这种情况，Web UI 会显示错误，并且您无法将该日程安排指派到该客户端。要解决此问题，请在指派日程安排时选中 **[取消受影响的操作]** 选项。这样就会取消以前安排的与新维护日程安排冲突的所有操作。

创建维护时段后，可以安排要在维护时段内执行的受限操作，例如软件包升级。

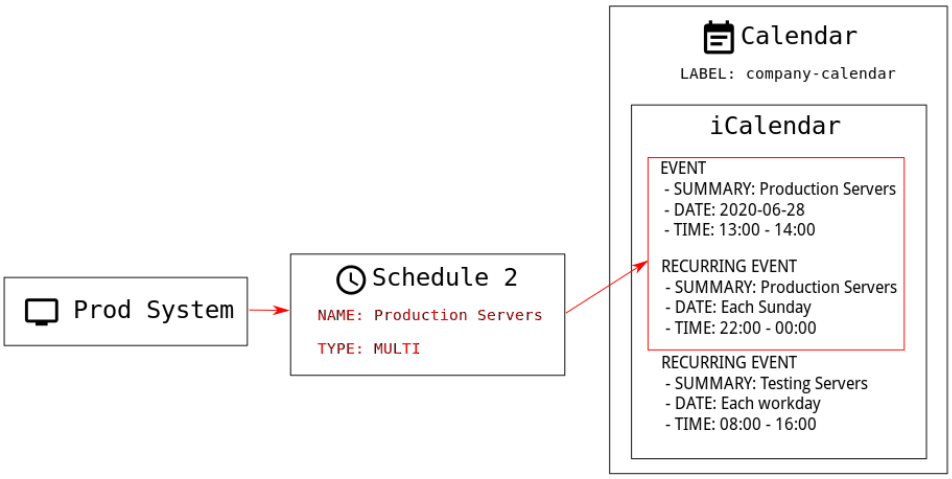
过程：安排软件包升级

1. 在 SUSE Manager Web UI 中，导航到**系统 › 系统列表**，选择要升级的客户端，然后转到**软件 › 软件包 › 升级**选项卡。
2. 从列表中选择要升级的软件包，然后单击 **[升级软件包]**。
3. 在维护时段字段中，选择由客户端用来执行升级的维护时段。
4. 单击 **[确认]** 以安排软件包升级。

14.1. 维护日程安排类型

创建日历时，该日历会包含许多事件，这些事件可能是一次性事件，也可能是重复性事件。每个事件包含一个摘要字段。如果您要为一个日历创建多个维护日程安排，可以使用摘要字段为每个日程安排指定事件。

例如，您可能想要为生产服务器创建一个日程安排，并为测试服务器创建另一个日程安排。在这种情况下，可以针对生产服务器的事件指定摘要：生产服务器，并针对测试服务器的事件指定摘要：测试服务器。



日程安排分为两种类型：“单”或“多”。如果您的日历包含应用于多个日程安排的事件，则您必须选择多，并确保根据日历文件中使用的摘要字段为日程安排命名。

过程：创建多日程安排

1. 在 SUSE Manager Web UI 中，导航到**日程安排 › 维护时段 › 日程安排**，然后单击 **[创建]**。
2. 在日程安排名称部分，键入日程安排的名称。 确保此名称与日历的摘要字段匹配。
3. 选中多选项。
4. 选择要指派到此日程安排的日历。
5. 单击 **[创建日程安排]** 以保存您的日程安排。
6. 要创建下一个日程安排，请单击 **[创建]**。
7. 在日程安排名称部分，键入第二个日程安排的名称。 确保此名称与第二个日历的摘要字段匹配。
8. 选中多选项。
9. 单击 **[创建日程安排]** 以保存您的日程安排。
10. 对需要创建的每个日程安排重复上述过程。

14.2. 受限制和非受限操作

本节包含受限和非受限操作的完整列表。

受限操作会对客户端进行重大修改，可能导致客户端停止运行。受限操作只能在维护时段内运行。受限操作包括：

- 软件包操作（例如安装、更新或去除软件包）
- 补丁更新
- 重引导客户端
- 回滚事务
- 配置管理更改任务

- 应用 Highstate（针对 Salt 客户端）
- 自动安装和重新安装
- 远程命令
- 产品迁移
- 群集操作

> 对于 Salt 客户端，可以随时通过导航到 **Salt › 远程命令**来直接运行远程命令。无论 Salt 客户端是否处于维护时段，都可以这样做。有关远程命令的详细信息，请参见 **Administration › Actions**。

非受限制操作属于次要操作，一般认为它们是安全的，不太可能会在客户端上造成问题。如果某个操作不受限制，则它在定义上就是非受限操作，随时都可以运行。

Chapter 15. 使用 mgr-sync

需要在命令提示符下使用 mgr-sync 工具。此工具提供用于操作 SUSE Manager 的功能，而 Web UI 不一定提供这些功能。mgr-sync 的主要用途是连接到 SUSE Customer Center，检索产品和软件包信息，并准备好要与 SUSE Manager Server 同步的通道。

此工具应与 SUSE 支持订阅配合使用。openSUSE、CentOS 和 Ubuntu 等开源发行套件不需要此工具。

下表中列出了 mgr-sync 的可用命令和参数。请对 mgr-sync 命令使用以下语法：

```
mgr-sync [-h] [--version] [-v] [-s] [-d {1,2,3}] {list,add,refresh,delete}
```

表格 3. mgr-sync 命令

命令	说明	示例用法
list	列出通道、组织身份凭证或产品	mgr-sync list channels
add	添加通道、组织身份凭证或产品	mgr-sync add channel <通道名称>
refresh	刷新产品、通道和订阅的本地副本	mgr-sync refresh
delete	从本地系统中删除现有的 SCC 组织身份凭证	mgr-sync delete credentials
sync	同步指定的通道，如果将通道名称留空，则请求提供名称	mgr-sync sync channel <通道名称>

要查看特定于某个命令的完整选项列表，请使用以下命令：

```
mgr-sync <命令> --help
```

表格 4. mgr-sync 可选参数

选项	选项缩写	说明	示例用法
help	h	显示命令用法和选项	mgr-sync --help
version	不适用	显示当前安装的 mgr-sync 版本	mgr-sync --version
verbose	v	提供详细输出	mgr-sync --verbose refresh
store-credentials	s	将身份凭证存储在本地隐藏文件中	mgr-sync --store -credentials
debug	d	记录附加调试信息。需要指定级别 1、2、3。3 提供的调试信息量最多	mgr-sync -d 3 refresh

选项	选项缩写	说明	示例用法
no-sync	不适用	与 `add` 命令结合使用，以添加产品或通道，而无需开始同步	`mgr-sync --no-sync add <通道名称>`

`mgr-sync` 的日志位于：

- `/var/log/rhn/mgr-sync.log`
- `/var/log/rhn/rhn_web_api.log`

Chapter 16. 使用 Prometheus 和 Grafana 进行监视

您可以使用 Prometheus 和 Grafana 监视 SUSE Manager 环境。SUSE Manager Server 和 Proxy 能够提供自我运行状况监视度量。您还可以在 Salt 客户端上安装和管理一些 Prometheus 导出器。

Prometheus 和 Grafana 软件包包含在以下发行套件的 SUSE Manager 客户端工具中：

- SUSE Linux Enterprise 12
- SUSE Linux Enterprise 15
- openSUSE Leap 15.x

需要在不包含 SUSE Manager Server 的计算机上安装 Prometheus 和 Grafana。我们建议使用受管 Salt SUSE 客户端作为监视服务器。不支持使用其他客户端作为监视服务器。

Prometheus 使用拉取机制提取度量，因此服务器必须能够与受监视客户端建立 TCP 连接。客户端上必须打开相应的端口，并且必须可以通过网络访问客户端。或者，您可以使用反向代理来建立连接。

> 对于您要监视的每个客户端，必须有一个监视附加订阅。访问 SUSE Customer Center 以管理您的 SUSE Manager 订阅。

16.1. Prometheus 和 Grafana

16.1.1. Prometheus

Prometheus 是一个开源监视工具，用于在时序数据库中记录实时度量。度量通过 HTTP 拉取，从而可以实现高性能和可伸缩性。

Prometheus 度量是时序数据，或者是属于同一个组或维度的带时间戳值。度量由其名称和一组标签唯一标识。

```
 度量名称          标签                时间戳    值
┌──────────────┬──────────────────────────────┐ ┌──────────────────────────────────────────┐
┌──────────────┬──────────┬──────────┐ ┌──────┐
http_requests_total{status="200", method="GET"} @1557331801.111  42236
```

每个受监视的应用程序或系统必须通过代码检测或 Prometheus 导出器按上述格式公开度量。

16.1.2. Prometheus 导出器

导出器是帮助将第三方系统中的度量作为 Prometheus 度量导出的库。每当无法直接使用 Prometheus 度量检测给定的应用程序或系统时，导出器就很有作用。可以在受监视主机上运行多个导出器以导出本地度量。

Prometheus 社区提供了官方导出器的列表，还有其他一些作为社区贡献内容提供的导出器。有关详细信息和导出器的详细列表，请参见 https://prometheus.io/docs/instrumenting/exporters/。

16.1.3. Grafana

Grafana 是一个数据可视化、监视和分析工具。它用于创建仪表板，其中的面板代表设置时间段内的特定度量。Grafana 通常与 Prometheus 一起使用，但也支持 ElasticSearch、MySQL、PostgreSQL 和 Influx DB 等其他数据源。有关 Grafana 的详细信息，请参见 https://grafana.com/docs/。

16.2. 设置监视服务器

要设置监视服务器，需要安装 Prometheus 和 Grafana 并对其进行配置。

16.2.1. 安装 Prometheus

如果您的监视服务器是 Salt 客户端，则您可以使用 SUSE Manager Web UI 安装 Prometheus 软件包。否则，可以在监视服务器上手动下载并安装该软件包。Prometheus 软件也可用于 SUSE Manager Proxy 和 SUSE Manager for Retail Branch Server。

> Prometheus 需要使用 POSIX 文件系统来存储数据。不支持不符合 POSIX 标准的文件系统，因此不支持 NFS 文件系统。

过程：使用 Web UI 安装 Prometheus

1. 在 SUSE Manager Web UI 中，打开要在其中安装 Prometheus 的系统的细节页面，然后导航到公式选项卡。
2. 选中 `Prometheus` 复选框以启用监视公式，然后单击 **[保存]**。
3. 在顶部菜单中导航到 `Prometheus` 选项卡。
4. 在 `SUSE Manager Server` 部分，输入有效的 SUSE Manager API 身份凭证。 确保您输入的身份凭证允许访问您要监视的系统集。
5. 根据需要自定义任何其他配置选项。
6. 单击 **[保存公式]**。
7. 应用 Highstate 并确认它成功完成。
8. 检查 Prometheus 界面是否正常加载。在浏览器中，使用端口 9090 导航到安装了 Prometheus 的服务器的 URL（例如 http://example.com:9090）。

有关监视公式的详细信息，请参见 **Specialized-guides › Salt**。

过程：手动安装和配置 Prometheus

1. 在监视服务器上，安装 `golang-github-prometheus-prometheus` 软件包：

```
zypper in golang-github-prometheus-prometheus
```

2. 启用 Prometheus 服务：

```
systemctl enable --now prometheus
```

3. 检查 Prometheus 界面是否正常加载。 在浏览器中，使用端口 9090 导航到安装了 Prometheus 的服务器的 URL（例如 http://example.com:9090）。

4. 打开配置文件 `/etc/prometheus/prometheus.yml` 并添加以下配置信息。 请将 `server.url` 替换为您的 SUSE Manager 服务器 URL，并调整 `username` 和 `password` 字段以便与您的 SUSE Manager 身份凭证匹配。

```
# {productname} self-health metrics
scrape_configs:
- job_name: 'mgr-server'
  static_configs:
    - targets:
      - 'server.url:9100'  # Node exporter
      - 'server.url:9187'  # PostgreSQL exporter
      - 'server.url:5556'  # JMX exporter (Tomcat)
      - 'server.url:5557'  # JMX exporter (Taskomatic)
      - 'server.url:9800'  # Taskomatic
    - targets:
      - 'server.url:80'    # Message queue
      labels:
        __metrics_path__: /rhn/metrics

# Managed systems metrics:
- job_name: 'mgr-clients'
  uyuni_sd_configs:
    - server: "http://server.url"
      username: "admin"
      password: "admin"
  relabel_configs:
    - source_labels: [__meta_uyuni_exporter]
      target_label: exporter
    - source_labels: [__address__]
      replacement: "No group"
      target_label: groups
    - source_labels: [__meta_uyuni_groups]
      regex: (.+)
      target_label: groups
    - source_labels: [__meta_uyuni_minion_hostname]
      target_label: hostname
    - source_labels: [__meta_uyuni_primary_fqdn]
      regex: (.+)
      target_label: hostname
    - source_labels: [hostname, __address__]
      regex: (.*);.*:(.*)
      replacement: ${1}:${2}
      target_label: __address__
    - source_labels: [__meta_uyuni_metrics_path]
      regex: (.+)
      target_label: __metrics_path__
    - source_labels: [__meta_uyuni_proxy_module]
      target_label: __param_module
    - source_labels: [__meta_uyuni_scheme]
      target_label: __scheme__
```

5. 保存该配置文件。

6. 重启动 Prometheus 服务：

```
systemctl restart prometheus
```

有关 Prometheus 配置选项的详细信息，请参见 https://prometheus.io/docs/prometheus/latest/configuration/configuration/ 上的 Prometheus 官方文档。

16.2.2. 安装 Grafana

如果您的监视服务器是 Salt 客户端，则您可以使用 SUSE Manager Web UI 安装 Grafana 软件包。否则，可以在监视服务器上手动下载并安装该软件包。

> 不可以在 SUSE Manager Proxy 上使用 Grafana。

过程：使用 Web UI 安装 Grafana

1. 在 SUSE Manager Web UI 中，打开要在其中安装 Grafana 的系统的细节页面，然后导航到公式选项卡。
2. 选中 `Grafana` 复选框以启用监视公式，然后单击 **[保存]**。
3. 在顶部菜单中导航到 `Grafana` 选项卡。
4. 在启用并配置 `Grafana`部分，输入用于登录 Grafana 的管理员身份凭证。
5. 在数据源部分，确保 Prometheus URL 字段指向运行 Prometheus 的系统。
6. 根据需要自定义任何其他配置选项。
7. 单击 **[保存公式]**。
8. 应用 Highstate 并确认它成功完成。
9. 检查 Grafana 界面是否正常加载。在浏览器中，使用端口 3000 导航到安装了 Grafana 的服务器的 URL（例如 http://example.com:3000）。

> SUSE Manager 为服务器自我运行状况监视度量、基本客户端监视等信息提供预构建的仪表板。您可以在公式配置页面中选择要置备的仪表板。

过程：手动安装 Grafana

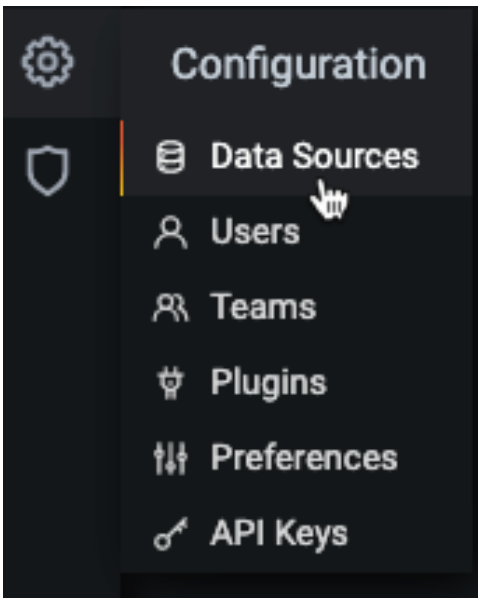
1. 安装 `grafana` 软件包：

```
zypper in grafana
```

2. 启用 Grafana 服务：

```
systemctl enable --now grafana-server
```

3. 在浏览器中，导航到安装了 Grafana 的服务器的 URL，使用端口 3000（例如 http://example.com:3000）。
4. 在登录页面中，输入 `admin` 作为用户名和口令。
5. 单击 **[登录]**。 如果成功登录，您将会看到要求您更改口令的提示。
6. 针对提示单击 **[确定]**，然后更改您的口令。
7. 将光标移到边栏菜单中的齿轮图标上，配置选项即会显示。



8. 单击 **[数据源]**。
9. 单击 **[添加数据源]** 会看到支持的所有数据源列表。
10. 选择 Prometheus 数据源。
11. 务必指定正确的 Prometheus 服务器 URL。
12. 单击 **[保存并测试]**。
13. 要导入仪表板，请单击边栏菜单中的 **[+]** 图标，然后单击 **[导入]**。
14. 对于 SUSE Manager 服务器概览，请加载仪表板 ID：`17569`。
15. 对于 SUSE Manager 客户端概览，请加载仪表板 ID：`17570`。

1. 有关监视公式的详细信息，请参见 **Specialized-guides › Salt**。
2. 有关如何手动安装和配置 Grafana 的详细信息，请参见 https://grafana.com/docs。

16.3. 配置 SUSE Manager 监视

在 SUSE Manager 4 和更高版本中，您可以让服务器公开 Prometheus 自我运行状况监视度量，并可以在客户端系统上安装和配置导出器。

16.3.1. 服务器自我监视

服务器自我运行状况监视度量涵盖了硬件、操作系统和 SUSE Manager 内部组件。这些度量是结合 Prometheus 导出器通过 Java 应用程序检测提供的。

SUSE Manager Server 随附了以下导出器软件包：

- Node 导出器：`golang-github-prometheus-node_exporter`。 请参见 https://github.com/prometheus/node_exporter。
- PostgreSQL 导出器：`prometheus-postgres_exporter`。 请参见 https://github.com/wrouesnel/postgres_exporter。
- JMX 导出器：`prometheus-jmx_exporter`。 请参见 https://github.com/prometheus/jmx_exporter。
- Apache 导出器：`golang-github-lusitaniae-apache_exporter`。 请参见 https://github.com/Lusitaniae/apache_exporter。

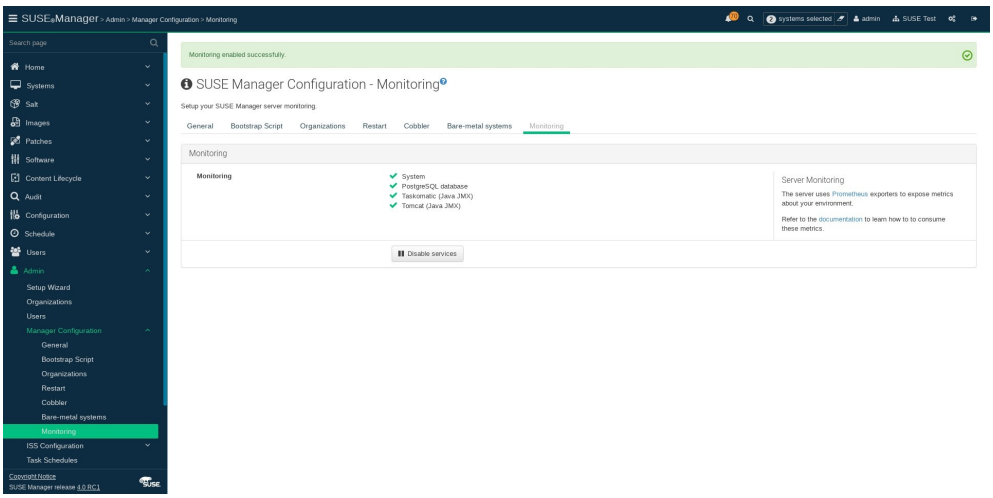
SUSE Manager Proxy 随附了以下导出器软件包：

- Node 导出器：`golang-github-prometheus-node_exporter`。 请参见 https://github.com/prometheus/node_exporter。
- Squid 导出器：`golang-github-boynux-squid_exporter`。 请参见 https://github.com/boynux/squid-exporter。

导出器软件包已预安装在 SUSE Manager Server 和 Proxy 中，但其各自的 systemd 守护程序默认已禁用。

过程：启用自我监视

1. 在 SUSE Manager Web UI 中，导航到**管理 › 管理器配置 › 监视**。
2. 单击 **[启用服务]**。
3. 重启动 Tomcat 和 Taskomatic。
4. 使用端口 9090 导航到 Prometheus 服务器的 URL（例如 http://example.com:9090）
5. 在 Prometheus UI 中，导航到**状态 › 目标**并确认 `mgr-server` 组中的所有端点都已启动。
6. 如果您还使用 Web UI 安装了 Grafana，则 SUSE Manager Server 仪表板上会显示服务器深入信息。



只能使用 Web UI 启用服务器自我运行状况监视。Prometheus 不会自动收集代理的度量。要在代理上启用自我运行状况监视，需要手动安装导出器并启用它们。

在 SUSE Manager 服务器上收集以下相关度量。

表格 5. 服务器统计数据（端口 80）

度量	类型	说明
uyuni_all_systems	计量器	所有系统数
uyuni_virtual_systems	计量器	虚拟系统数
uyuni_inactive_systems	计量器	非活动系统数
uyuni_outdated_systems	计量器	安装了过时软件包的系统数

表格 6. PostgreSQL 导出器（端口 9187）

度量	类型	说明
pg_stat_database_tup_fetched	计数器	查询提取的行数
pg_stat_database_tup_inserted	计数器	查询插入的行数
pg_stat_database_tup_updated	计数器	查询更新的行数
pg_stat_database_tup_deleted	计数器	查询删除的行数
mgr_serveractions_completed	计量器	完成的操作数
mgr_serveractions_failed	计量器	失败的操作数
mgr_serveractions_picked_up	计量器	拾取的操作数
mgr_serveractions_queued	计量器	排队的操作数

表格 7. JMX 导出器（Tomcat 端口 5556、Taskomatic 端口 5557）

度量	类型	说明
java_lang_Threading_ThreadCount	计量器	活动线程数
java_lang_Memory_HeapMemoryUsage_used	计量器	当前堆内存使用量

表格 8. 服务器消息队列（端口 80）

度量	类型	说明
message_queue_thread_pool_threads	计数器	到目前为止创建的消息队列线程数
message_queue_thread_pool_threads_active	计量器	当前处于活动状态的消息队列线程数
message_queue_thread_pool_task_count	计数器	到目前为止提交的任务数
message_queue_thread_pool_completed_task_count	计数器	到目前为止完成的任务数

表格 9. Salt 队列（端口 80）

度量	类型	说明
salt_queue_thread_pool_size	计量器	每个 Salt 队列创建的线程数
salt_queue_thread_pool_active_threads	计量器	每个队列当前处于活动状态的 Salt 线程数
salt_queue_thread_pool_task_total	计数器	每个队列已提交的任务数
salt_queue_thread_pool_completed_task_total	计数器	每个队列已完成的任务数

每个 salt_queue 值都有一个名为 `queue` 值为队列编号的标签。

表格 10. Taskomatic 日程安排程序（端口 9800）

度量	类型	说明
taskomatic_scheduler_threads	计数器	到目前为止创建的日程安排程序线程数
taskomatic_scheduler_threads_active	计量器	当前处于活动状态的日程安排程序线程数
taskomatic_scheduler_completed_task_count	计数器	到目前为止完成的任务数

16.3.2. 监视受管系统

可以使用公式在 Salt 客户端上安装和配置 Prometheus 度量导出器。这些软件包可以从 SUSE Manager 客户端工具通道获得，并且可以直接在 SUSE Manager Web UI 中启用和配置。

可将这些导出器安装在受管系统上：

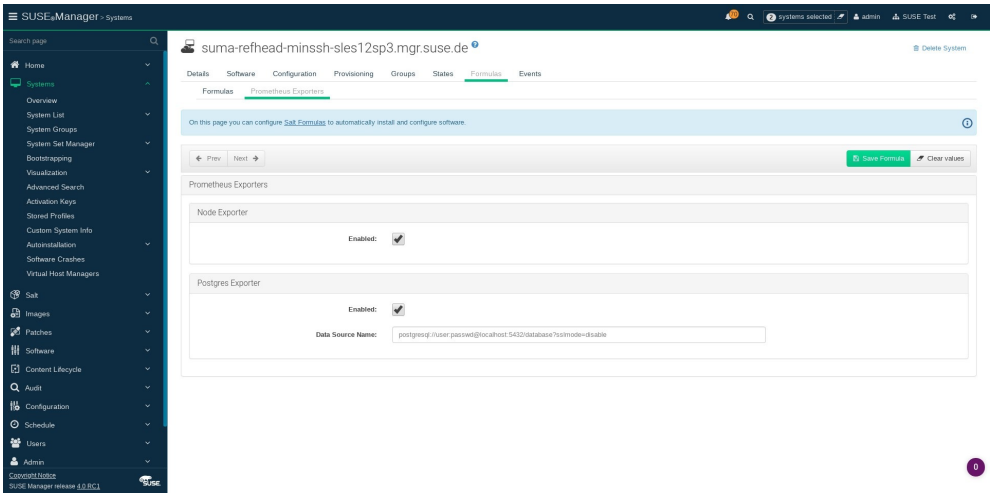
- Node 导出器：`golang-github-prometheus-node_exporter`。 请参见 https://github.com/prometheus/node_exporter。
- PostgreSQL 导出器：`prometheus-postgres_exporter`。 请参见 https://github.com/wrouesnel/postgres_exporter。
- Apache 导出器：`golang-github-lusitaniae-apache_exporter`。 请参见 https://github.com/Lusitaniae/apache_exporter。

在 SLE Micro 上，只能使用 Node Exporter 和 Blackbox Exporter。

安装并配置导出器后，您可以开始使用 Prometheus 从受监视系统收集度量。如果您已使用 Web UI 配置了监视服务器，则会自动收集度量。

过程：在客户端上配置 Prometheus 导出器

1. 在 SUSE Manager Web UI 中，打开要监视的客户端的细节页面，并导航到**公式**选项卡。
2. 选中 `Prometheus 导出器`公式对应的`已启用`复选框。
3. 单击 **[保存]**。
4. 导航到**公式 › Prometheus 导出器**选项卡。
5. 选择要启用的导出器并根据需要自定义参数。 `地址`字段接受冒号开头的端口号 (`:9100`) 或完全可解析的地址 (`example:9100`)。
6. 单击 **[保存公式]**。
7. 应用 Highstate。



还可为系统组配置监视公式，只需应用相应组中各个系统使用的同一种配置即可。

有关监视公式的详细信息，请参见 **Specialized-guides › Salt**。

16.3.3. 更改 Grafana 口令

要更改 Grafana 口令，请按照 Grafana 文档中所述的步骤操作：

- https://grafana.com/docs/grafana/latest/administration/user-management/user-preferences/#change-your-grafana-password

如果您忘记了 Grafana 管理员口令，可以使用以下命令将其重设置为 `root`：

```
grafana-cli --configOverrides cfg:default.paths.data=/var/lib/grafana --homepath
/usr/share/grafana admin reset-admin-password <新口令>
```

16.4. 网络边界

Prometheus 使用拉取机制提取度量，因此服务器必须能够与受监视客户端建立 TCP 连接。Prometheus 默认使用以下端口：

- Node 导出器：9100
- PostgreSQL 导出器：9187
- Apache 导出器：9117

此外，如果您不是在运行 Prometheus 的同一台主机上运行警报管理器，则还需要在所在主机上打开端口 9093。

对于安装在云实例上的客户端，可以将所需的端口添加到有权访问监视服务器的安全组中。

或者，可以在导出器的本地网络中部署 Prometheus 实例，并配置联合。这样，主监视服务器就能从本地 Prometheus 实例中抓取时序。如果您使用此方法，只需要打开 Prometheus API 端口 (9090) 即可。

有关 Prometheus 联合的详细信息，请参见 https://prometheus.io/docs/prometheus/latest/federation/。

您还可以通过网络边界来中转请求。PushProx 等工具会在网络屏障的两端部署代理和客户端，并允许 Prometheus 跨网络拓扑（例如 NAT）工作。

有关 PushProx 的详细信息，请参见 https://github.com/RobustPerception/PushProx。

16.4.1. 反向代理设置

Prometheus 使用拉取机制提取度量，因此服务器必须能够与受监视客户端上的每个导出器建立 TCP 连接。为了简化防火墙配置，可为导出器使用反向代理，以便在单个端口上公开所有度量。

过程：安装使用反向代理的 Prometheus 导出器

1. 在 SUSE Manager Web UI 中，打开要监视的系统的细节页面，并导航到公式选项卡。
2. 选中 `Prometheus 导出器`复选框以启用导出器公式，然后单击 **[保存]**。

3. 在顶部菜单中导航到 `Prometheus 导出器`选项卡。
4. 选中`启用反向代理`选项，并输入有效的反向代理端口号。 例如 `9999`。
5. 根据需要自定义其他导出器。
6. 单击 **[保存公式]**。
7. 应用 Highstate 并确认它成功完成。

有关监视公式的详细信息，请参见 **Specialized-guides › Salt**。

16.5. 安全

Prometheus 服务器和 Prometheus Node 导出器提供内置机制用于通过 TLS 加密和身份验证来保护其端点。SUSE Manager Web UI 简化了所有相关组件的配置。TLS 证书必须由用户提供和部署。在 SUSE Manager 中可以启用以下安全模型：

- Node 导出器：TLS 加密和基于客户端证书的身份验证
- Prometheus：TLS 加密和基本身份验证

有关配置所有可用选项的详细信息，请参见 **Specialized-guides › Salt**。

16.5.1. 生成 TLS 证书

默认情况下，SUSE Manager 不提供任何用于保护监视配置的证书。为了提供安全性，您可以生成或导入自定义证书，包括自我签名证书或由第三方证书颁发机构 (CA) 签名的证书。

本章说明如何为使用 SUSE Manager CA 自我签名的 Prometheus 和 Node 导出器受控端生成客户端/服务器证书。

过程：创建服务器/客户端 TLS 证书

1. 在 SUSE Manager Server 上的命令提示符下运行以下命令：

```
rhn-ssl-tool --gen-server --dir="/root/ssl-build" --set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname="minion.example.com" --set-cname="minion.example.com" --no-rpm
```

   确保 `set-cname` 参数是您的 Salt 客户端的完全限定域名 (FQDN)。如果需要多个别名，可以多次使用 `set-cname` 参数。

2. 将 `server.crt` 和 `server.key` 文件复制到 Salt 受控端，并为 `prometheus` 用户提供读取访问权限。

Chapter 17. 组织

组织用于管理 SUSE Manager 中的用户访问权限和许可权限。

对于大多数环境而言，一个组织便已足够。但是，较复杂的环境可能需要多个组织。您可以为企业中的每个物理位置或不同的业务职能创建一个组织。

创建组织后，可以创建用户并将其指派到组织。然后，可以在组织级别指派权限，这些权限默认将应用于指派到组织的每个用户。

您还可以为新组织配置身份验证方法，包括 PAM 和单点登录。有关身份验证的详细信息，请参见 **Administration › Auth-methods**。

您必须以 SUSE Manager 管理员身份登录才能创建和管理组织。

过程：创建新组织

1. 在 SUSE Manager Web UI 中，导航到**管理 › 组织**，然后单击 **[创建组织]**。
2. 在创建组织对话框中填写以下字段：
   - 在组织名称字段中，键入新组织的名称。 该名称的长度应为 3 到 128 个字符。
   - 在要使用的登录名字段中，键入要用于组织管理员的登录名。 这必须是一个新的管理员帐户，您无法使用现有的管理员帐户（包括当前使用的登录帐户）登录到新组织。
   - 在要使用的口令字段中，键入新组织管理员的口令。 在确认口令字段中再次键入该口令以确认。口令强度由口令字段下方的彩色条指示。
   - 在电子邮件字段中，键入新组织管理员的电子邮件地址。
   - 在名字字段中选择一种称呼，然后键入新组织管理员的名字。
   - 在姓氏字段中，键入新组织管理员的姓氏。
3. 单击 **[创建组织]**。

17.1. 管理组织

在 SUSE Manager Web UI 中，导航到**管理 › 组织**可查看可用组织的列表。单击某个组织的名称可对其进行管理。

在**管理 › 组织**部分，可以访问相应的选项卡来管理组织的用户、信任、配置和状态。

组织只能由其管理员管理。要管理组织，请确保以您要更改的组织的正确管理员身份登录。

17.1.1. 组织用户

导航到用户选项卡可查看与组织关联的所有用户的列表及其角色。单击某个用户名会转到用户菜单，可在其中添加、更改或删除用户。

17.1.2. 受信任组织

导航到信任选项卡可添加或去除受信任组织。在组织之间建立信任可让它们相互共享内容，这样您也可以在不同的组织之间切换客户端。

17.1.3. 配置组织

导航到配置选项卡可以管理组织的配置。这包括使用暂存内容和使用 SCAP 文件。

有关内容暂存的详细信息，请参见 **Administration › Content-staging**。

有关 OpenSCAP 的详细信息，请参见 **Reference › Audit**。

17.2. 管理状态

导航到状态选项卡可以管理组织中所有客户端的 Salt 状态。使用状态可以定义全局安全策略，或者将公共管理员用户添加到所有客户端。

有关 Salt 状态的详细信息，请参见 **Specialized-guides › Salt**。

17.2.1. 管理配置通道

可以选择要在整个组织中应用哪些配置通道。可以在 SUSE Manager Web UI 中导航到**配置 › 通道**来创建配置通道。使用 SUSE Manager Web UI 将配置通道应用于您的组织。

过程：将配置通道应用于组织

1. 在 SUSE Manager Web UI 中，导航到**首页 › 我的组织 › 配置通道**。
2. 使用搜索功能按名称查找通道。
3. 选中要应用的通道，然后单击 **[保存更改]**。 这会将更改保存到数据库，但不会将其应用于通道。
4. 单击 **[应用]** 以应用更改。 随即会安排将更改应用于组织中的所有客户端的任务。

Chapter 18. 补丁管理

本章包含有关补丁管理的各个主题。

18.1. 已收回补丁

在供应商发布某个新补丁后，该补丁在某种情况下可能会产生不利的负面影响（在安全性、稳定性方面），而这种情况并未通过测试识别出来。如果出现这种情况（非常罕见），供应商通常会发布新补丁，此过程可能需要数小时甚至数日时间，具体取决于该供应商实施的内部流程。

SUSE 引入了一个称为已收回补丁的新机制（2021），可以通过将此类补丁的建议状态设置为已收回（而不是最终或稳定）来近实时地撤消这些补丁。

> 如果某个补丁的建议状态属性设置为 `retracted`，则会收回该补丁。如果某个软件包属于已收回的补丁，则会收回该软件包。

无法在包含 SUSE Manager 的系统上安装已收回的补丁或软件包。安装已收回软件包的唯一方法是使用 `zypper install` 并指定确切的软件包版本来手动安装。例如：

```
zypper install vim-8.0.1568-5.14.1
```

SUSE Manager Web UI 中的 ⊗ 图标描绘了补丁和软件包的已收回状态。例如，查看：

- 通道中软件包的列表
- 通道中补丁的列表

收回安装在系统上的补丁或软件包时，⊗ 图标也会显示在该系统的已安装软件包列表中。SUSE Manager 不提供降级此类补丁或软件包的方法。

18.1.1. 通道克隆

使用克隆的通道时，必须小心将原始通道的已收回建议状态传播到克隆版本。

将供应商通道克隆到组织中时，也会克隆通道补丁。

当供应商收回通道中的补丁并且 SUSE Manager 同步此通道（例如，通过夜间作业）时，`retracted` 属性不会传播到克隆的补丁，并且订阅克隆通道的客户端看不到该属性。要将该属性传播到克隆的通道，请使用以下方法之一：

- 补丁同步（**软件 › 管理 › 克隆的通道 › 补丁 › 同步**）。使用此功能可使克隆通道中补丁的属性与其原始通道保持一致。
- 内容生命周期管理。有关内容生命周期管理上下文中克隆的通道的详细信息，请参见 **Client-configuration › Channels**。

18.1.2. 补丁共享

当您在组织中创建多个供应商通道克隆版本时，补丁不会克隆多次，而是在克隆的通道之间共享。因此，当您同步克隆的补丁时（使用补丁同步功能或上面提到的内容生命周期管理），使用该克隆补丁的所有通道都会看到这种变化。

示例：

1. 假设有两个内容生命周期管理项目：`prj1` 和 `prj2`
2. 这两个项目都有 2 个环境：`dev` 和 `test`
3. 这两个项目都有一个设置为源通道的供应商通道
4. 此场景中的所有通道（总共四个克隆的通道）与供应商通道的最新状态相一致
5. 供应商收回源通道中的某个补丁，夜间作业将此补丁同步到 SUSE Manager
6. 四个通道都看不到这种变化，因为它们使用的是补丁克隆版本，而不是直接使用该补丁。
7. 在您同步补丁（构建这两个项目中的任何一个，或者对四个克隆通道中的任何一个使用补丁同步功能）后，由于补丁共享的原因，*所有*克隆的通道都会发现该补丁已收回。

Chapter 19. 生成报告

SUSE Manager 允许用户生成各种报告。这些报告有助于清点已订阅的系统、用户和组织。使用报告通常比从 SUSE Manager Web UI 手动收集信息更方便，尤其是要管理众多的系统时。

虽然可以使用命令行工具 `spacewalk-report` 生成预配置的报告，但随着**Specialized-guides › Large-deployments**的引入，也可以生成完全自定义的报告。可以通过将任何支持 SQL 语言的报告工具连接到报告数据库并直接提取数据来实现此目的。有关数据可用性和结构的详细信息，请参见报告数据库纲要文档。

19.1. 使用 spacewalk-report

要生成报告，必须安装 `spacewalk-reports` 软件包。使用 `spacewalk-report` 命令可以组织和显示有关整个 SUSE Manager 中的内容、系统和用户资源的报告。

> 由于**Specialized-guides › Large-deployments**的引入，`spacewalk-report` 现在默认会从报告数据库中收集数据。有关详细信息，请参见 spacewalk-report 和报告数据库。

可以针对以下各项生成报告：

1. 系统库存：列出所有已注册到 SUSE Manager 的系统。
2. 补丁：列出所有与已注册系统相关的补丁。 可以按严重性以及适用于特定补丁的系统将补丁排序。
3. 用户：列出所有已注册用户以及与特定用户关联的所有系统。

要获取 CSV 格式的报告，请在服务器上的命令提示符下运行以下命令：

```
spacewalk-report <报告名称>
```

19.2. spacewalk-report 和报告数据库

`spacewalk-report` 默认使用新的报告数据库来提取数据。这意味着，新生成的报告在数据结构和格式方面存在一定的差异。所有报告的共同差异是：

- 报告数据不会实时更改，而只能通过执行安排的任务来更新；
- 已去除重复数据，以前被视为“多值”的列现在包含多个由 `;` 分隔的值。这也意味着命令行选项 `--multival-on-rows` 和 `--multival-separator` 不再适用于新报告，因为它们的行为现在是默认行为；
- 在所有报告中引入了新列 `mgm_id` 和 `synced_date`，以标识中心方案中的管理服务器，以及上次从应用程序数据库更新信息的时间；
- 现在，所有布尔值都由 `True`/`False` 表示，而不是由 `1`/`0` 值表示；
- `org_id` 列已由 `organization` 取代，后者包含组织名称而不是数字标识符；
- “server”一词已由“system”取代。因此，举例而言，`server_id` 列现在名为 `system_id`。

有关特定于报告的更改，请参见可用报告列表。

> 如果这种行为更改造成了问题，可以使用新选项 `--legacy-report` 回退到针对应用程序数据库执行的旧报告。

有关中心报告的详细信息，请参见 **Specialized-guides › Large-deployments**。

19.3. 可用报告列表

下表列出了可用报告：

表格 11. spacewalk-report 报告

报告	调用方式	说明	使用报告数据库	具体差异
操作	actions	所有操作。	是	id 列现在名为 action_id
激活密钥	activation-keys	所有激活密钥，及其关联的权利、通道、配置通道、系统组和软件包。	否	
激活密钥：通道	activation-keys-channels	所有激活密钥以及与每个密钥关联的实体。	否	
激活密钥：配置	activation-keys-config	所有激活密钥以及与每个密钥关联的配置通道。	否	
激活密钥：服务器组	activation-keys-groups	所有激活密钥以及与每个密钥关联的系统组。	否	
激活密钥：软件包	activation-keys-packages	所有激活密钥以及每个密钥可部署的软件包。	否	
通道软件包	channel-packages	通道中的所有软件包。	是	
通道报告	channels	给定通道的详细报告。	是	
克隆的通道报告	cloned-channels	克隆的通道的详细报告。	是	
配置文件	config-files	所有组织的所有配置文件修订，包括文件内容和文件信息。	否	

报告	调用方式	说明	使用报告数据库	具体差异
最新配置文件	`config-files-latest`	所有组织的最近配置文件修订，包括文件内容和文件信息。	否	
自定义通道	`custom-channels`	特定组织拥有的所有通道的通道元数据。	是	`id` 列现在名为 `channel_id`
自定义信息	`custom-info`	客户端自定义信息。	是	
补丁通道	`errata-channels`	通道中的所有补丁。	是	
补丁细节	`errata-list`	影响已注册客户端的所有补丁。	是	
所有补丁	`errata-list-all`	所有补丁。	否	
适用于客户端的补丁	`errata-systems`	适用的补丁，以及受影响的所有已注册客户端。	是	
主机 Guest	`host-guests`	主机和 Guest 映射。	是	
非活动客户端	`inactive-systems`	非活动客户端。	是	必需的参数现在名为 `threshold`。
系统库存	`inventory`	已注册到服务器的客户端，以及硬件和软件信息。	是	已去除 `osad_status` 列。
Kickstart 脚本	`kickstart-scripts`	所有 Kickstart 脚本和细节。	否	
Kickstart 树	`kickstartable-trees`	可无人值守安装树。	否	"
所有可升级版本	`packages-updates-all`	所有可升级的较新软件包版本。	是	
最新可升级版本	`packages-updates-newest`	可升级的最新软件包版本。	是	
代理概览	`proxies-overview`	所有代理，以及已注册到每个代理的客户端。	是	
储存库	`repositories`	所有储存库及其关联的 SSL 细节，以及所有过滤器。	否	
SCAP 结果	`scap-scan`	OpenSCAP `sccdf` 评估结果。	是	

报告	调用方式	说明	使用报告数据库	具体差异
SCAP 结果	scap-scan-results	OpenSCAP sccdf 评估结果，采用不同的格式。	是	
系统数据	splice-export	Splice 集成所需的客户端数据。	否	
系统通用性	system-currency	每个已注册客户端的可用补丁数。	否	
系统额外软件包	system-extra-packages	所有客户端上已安装的、无法从客户端订阅的通道中使用的所有软件包。	是	
系统组	system-groups	系统组。	是	
系统组的激活密钥	system-groups-keys	系统组的激活密钥。	否	
系统组中的系统	system-groups-systems	系统组中的客户端。	是	
系统组用户	system-groups-users	系统组以及对其拥有权限的用户。	否	
历史记录：系统	system-history	每个客户端的事件历史记录。	是	
历史记录：通道	system-history-channels	通道事件历史记录。	是	
历史记录：配置	system-history-configuration	配置事件历史记录。	是	已去除 created_date 列。
历史记录：权利	system-history-entitlements	系统权利事件历史记录。	是	
历史记录：勘误	system-history-errata	勘误事件历史记录。	是	已去除 created_date 列。
历史记录：Kickstart	system-history-kickstart	Kickstart 事件历史记录。	是	已去除 created_date 列。
历史记录：软件包	system-history-packages	软件包事件历史记录。	是	已去除 created_date 列。
历史记录：SCAP	system-history-scap	OpenSCAP 事件历史记录。	是	已去除 created_date 列。
MD5 证书	system-md5-certificates	所有使用带有 MD5 校验和的证书的已注册客户端。	否	

报告	调用方式	说明	使用报告数据库	具体差异
安装的软件包	`system-packages-installed`	客户端上安装的软件包。	是	
系统配置文件	`system-profiles`	所有已注册到服务器的客户端，以及硬件和软件组信息。	否	
用户	`users`	所有已注册到 SUSE Manager 的用户。	是	已去除 `organization_id` 列。
MD5 用户	`users-md5`	所有组织的使用 MD5 已加密口令的所有用户及其细节和角色。	是	已去除 `organization_id` 列。
管理的系统	`users-systems`	单个用户可管理的客户端。	是	已去除 `organization_id` 列。

如需单个报告的详细信息，请运行 `spacewalk-report` 并指定选项 `--info` 或 `--list-fields-info` 和报告名称。这会显示该报告中可用字段的说明和列表。

有关程序调用和选项的更多信息，请参见 `spacewalk-report(8)` 手册页以及 `spacewalk-report` 命令的 `--help` 参数。

Chapter 20. 安全

20.1. 设置用于客户端到主控端验证的指纹

在高度安全的网络配置中，您可能希望确保您的 Salt 客户端连接特定的主控端。要设置从客户端到主控端的验证，请在 `/etc/salt/minion` 配置文件中输入主控端的指纹。具体请参见以下过程：

过程：将主控端的指纹添加到客户端

1. 在主控端的命令提示符下，以 root 身份使用以下命令查找 `master.pub` 指纹：

   ```
   salt-key -F master
   ```

   在客户端打开 `/etc/salt/minion` 配置文件。取消注释下面一行并输入主控端的指纹（请替换下面的示例指纹）：

   ```
   master_finger: 'ba:30:65:2a:d6:9e:20:4f:d8:b2:f3:a7:d4:65:11:13'
   ```

2. 重启动 salt-minion 服务：

   ```
   # systemctl restart salt-minion
   ```

有关从客户端配置安全性的信息，请参见 https://docs.saltstack.com/en/latest/ref/configuration/minion.html。

20.2. 为储存库元数据签名

需有一个自定义 GPG 密钥才能为储存库元数据签名。

过程：生成自定义 GPG 密钥

1. 以 root 用户身份使用 `gpg` 命令生成新密钥：

   ```
   gpg --gen-key
   ```

2. 根据提示选择 `RSA` 作为密钥类型，将大小指定为 2048 位，并为密钥选择适当的失效日期。 检查新密钥的细节，然后键入 `y` 以确认。
3. 根据提示输入要与该密钥关联的名称和电子邮件地址。 如果需要，您还可以添加注释以帮助识别该密钥。 如果您对用户身份设置感到满意，请键入 `O` 以确认。
4. 根据提示输入通行口令以保护您的密钥。
5. 该密钥应自动添加到您的密钥环。 可以通过列出密钥环中的密钥进行检查：

   ```
   gpg --list-keys
   ```

6. 在文本编辑器中打开 `/etc/rhn/signing.conf` 配置文件并添加下面一行内容，将密钥环的口令添加到该文件：

```
GPGPASS="password"
```

有关如何续订 GPG 密钥，请参见 **Administration › Troubleshooting**。

可以在命令行中使用 `mgr-sign-metadata-ctl` 命令来管理元数据签名。

过程：启用元数据签名

1. 您需要知道所要使用的密钥的短标识符。 可以简短格式列出可用的公共密钥：

```
gpg --keyid-format short --list-keys
...
pub   rsa2048/3E7BFE0A 2019-04-02 [SC] [expires: 2021-04-01]
      A43F9EC645ED838ED3014B035CFA51BF3E7BFE0A
uid         [ultimate] SUSE Manager
sub   rsa2048/118DE7FF 2019-04-02 [E] [expires: 2021-04-01]
```

2. 使用 `mgr-sign-metadata-ctl` 命令启用元数据签名：

```
mgr-sign-metadata-ctl enable 3E7BFE0A
OK. Found key 3E7BFE0A in keyring.
DONE. Set key 3E7BFE0A in /etc/rhn/signing.conf.
DONE. Enabled metadata signing in /etc/rhn/rhn.conf.
DONE. Exported key 4E2C3DD8 to /srv/susemanager/salt/gpg/mgr-keyring.gpg.
DONE. Exported key 4E2C3DD8 to /srv/www/htdocs/pub/mgr-gpg-pub.key.
NOTE. For the changes to become effective run:
  mgr-sign-metadata-ctl regen-metadata
```

3. 可以使用以下命令检查您的配置是否正确：

```
mgr-sign-metadata-ctl check-config
```

4. 重启动服务并安排元数据重新生成以应用更改：

```
mgr-sign-metadata-ctl regen-metadata
```

还可以使用 `mgr-sign-metadata-ctl` 命令执行其他任务。使用 `mgr-sign-metadata-ctl --help` 可查看完整列表。

储存库元数据签名是全局选项。启用后，将对服务器上的所有软件通道启用该选项。这意味着，连接到服务器的所有客户端需要信任新的 GPG 密钥才能安装或更新软件包。

过程：在客户端上导入 GPG 密钥

1. 将 GPG 密钥部署到客户端的过程适用于 Salt 状态。
2. 使用 SUSE Manager Web UI 应用 Highstate。

有关 GPG 密钥查错的详细信息，请参见 **Administration › Troubleshooting**。

20.3. 镜像源软件包

如果您在本地构建自己的软件包，或者出于法律原因需要提供软件包的源代码，可以在 SUSE Manager Server 上镜像源软件包。

镜像源软件包可能会消耗大量磁盘空间。

过程：镜像源软件包

1. 打开 `/etc/rhn/rhn.conf` 配置文件并添加下面一行内容：

```
server.sync_source_packages = 1
```

2. 重启动 Spacewalk 服务以应用更改：

```
spacewalk-service restart
```

目前，只能为所有储存库全局启用此功能。无法选择单个要镜像的储存库。

激活此功能后，源软件包会在下次储存库同步后显示在 SUSE Manager Web UI 中。它们显示为二进制软件包的源，可以直接从 Web UI 下载。无法使用 Web UI 在客户端上安装源软件包。

20.4. 使用 OpenSCAP 确保系统安全

SUSE Manager 使用 OpenSCAP 来审计客户端。它允许您为任何客户端安排合规性扫描并查看扫描结果。

20.4.1. 关于 SCAP

安全内容自动化协议 (SCAP) 是根据社区观点衍生出的一套综合性可互操作规范。它是由美国国家标准与技术研究院 (NIST) 维护的一系列规范，用于维持企业系统的系统安全性。

制定 SCAP 的目的是提供一种标准化方法来维持系统安全性，并且使用的标准会根据社区和企业的需求不断变化。新规范根据 NIST 的 SCAP 发布周期进行控制，以提供一致且可重复的修订工作流程。有关详细信息，请参见：

- http://scap.nist.gov/timeline.html
- https://csrc.nist.gov/projects/security-content-automation-protocol
- https://www.open-scap.org/features/standards/
- https://ncp.nist.gov/repository?scap

SUSE Manager 使用 OpenSCAP 来实现 SCAP 规范。OpenSCAP 是一个利用可扩展配置清单描述格式 (XCCDF) 的审计工具。XCCDF 是表达清单内容和定义安全清单的标准方式。它还结合了其他规范，例如通用平台枚举

(CPE)、通用配置枚举 (CCE) 及开放漏洞和评估语言 (OVAL)，以创建 SCAP 表达的、可由 SCAP 验证过的产品处理的清单。

OpenSCAP 使用 SUSE 安全团队生成的内容来验证补丁是否存在。OpenSCAP 使用基于标准和规范的规则来检查系统安全配置设置，并检查系统是否存在遭受入侵的迹象。有关 SUSE 安全团队的详细信息，请参见 https://www.suse.com/support/security。

20.4.2. 为客户端的 SCAP 扫描做好准备

在开始之前，需要为客户端系统的 SCAP 扫描做好准备。

OpenSCAP 审计在使用 SSH 联系方法的 Salt 客户端上不可用。

扫描客户端可能会消耗被扫描客户端的大量内存和计算能力。对于 Red Hat 客户端，请确保每个要扫描的客户端上至少有 2 GB 可用 RAM。

对于传统客户端和 Salt 客户端，请在开始之前安装 OpenSCAP 扫描程序和 SCAP 安全指南（内容）软件包。根据操作系统，这些软件包要么包含在基本操作系统中，要么包含在 SUSE Manager 客户端工具中。

下表根据客户端操作系统列出了所需的软件包：

表格 12. OpenSCAP 软件包

操作系统	扫描程序	内容
SLES	openscap-utils	scap-security-guide
openSUSE	openscap-utils	scap-security-guide
RHEL	openscap-utils	scap-security-guide-redhat
CentOS	openscap-utils	scap-security-guide-redhat
Oracle Linux	openscap-utils	scap-security-guide-redhat
Ubuntu	libopenscap8	scap-security-guide-ubuntu
Debian	libopenscap8	scap-security-guide-debian

RHEL 7 和兼容系统提供了一个 `scap-security-guide` 软件包，其中包含已过时的内容。建议您使用 SUSE Manager 客户端工具中的 `scap-security-guide-redhat` 软件包。

SUSE 为不同的 openscap 配置文件提供了 `scap-security-guide` 软件包。在当前版本的 `scap-security-guide` 中，SUSE 支持以下配置文件：

- 适用于 SUSE Linux Enterprise Server 12 和 15 的 DISA STIG 配置文件
- 适用于 SUSE Linux Enterprise Server 12 和 15 的 ANSSI-BP-028 配置文件
- 适用于 SUSE Linux Enterprise Server 12 和 15 的 PCI-DSS 配置文件
- 适用于 SUSE Linux Enterprise Server 15 的 HIPAA 配置文件
- 适用于 SUSE Linux Enterprise Server 12 和 15 的 CIS 配置文件
- 强化 SUSE Linux Enterprise Server for SAP Applications 15 的公有云映像
- SUSE Linux Enterprise 15 的公有云强化
- SLE 12 和 15 的标准系统安全性配置文件

此处未列出的其他配置文件由社区提供，SUSE 不为其提供官方支持。

对于非 SUSE 操作系统，包含的配置文件由社区提供。SUSE 不为其提供官方支持。

20.4.3. OpenSCAP 内容文件

OpenSCAP 使用 SCAP 内容文件来定义测试规则。这些内容文件是根据 XCCDF 或 OVAL 标准创建的。除了 SCAP 安全指南之外，您还可以下载公开的内容文件并根据要求对其进行自定义。可为默认内容文件模板安装 SCAP 安全指南软件包。或者，如果您熟悉 XCCDF 或 OVAL 的话，可以创建自己的内容文件。

我们建议您使用模板来创建自己的 SCAP 内容文件。如果您创建并使用自己的自定义内容文件，需要自负风险。如果您的系统因使用自定义内容文件而损坏，SUSE 可能不会为您提供支持。

创建内容文件后，需要将该文件传输到客户端。可以像移动任何其他文件一样，使用物理存储媒体传输该文件，或者使用 Salt（例如 salt-cp 或 Salt 文件服务器）在网络上通过 `ftp` 或 `scp` 传输该文件。

我们建议您创建一个软件包以将内容文件分发到使用 SUSE Manager 管理的客户端。可将软件包签名并对其进行校验以确保其完整性。有关详细信息，请参见 **Administration › Custom-channels**。

20.4.4. 查找 OpenSCAP 配置文件

不同的操作系统提供不同的 OpenSCAP 内容文件和配置文件。一个内容文件可以包含多个配置文件。

在基于 RPM 的操作系统上，可使用以下命令确定可用 SCAP 文件的位置：

```
rpm -ql <表中的 SCAP 安全指南软件包名称>
```

在基于 DEB 的操作系统上，可使用以下命令确定可用 SCAP 文件的位置：

```
dpkg -L <表中的 SCAP 安全指南软件包名称>
```

确定了一个符合您需求的 SCAP 内容文件后，列出客户端上可用的配置文件：

```
oscap info /usr/share/xml/scap/ssg/content/ssg-sle15-ds-1.2.xml
Document type: Source Data Stream
Imported: 2021-03-24T18:14:45

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-sle15-xccdf-1.2.xml
Generated: (null)
Version: 1.2
Checklists:
    Ref-Id: scap_org.open-scap_cref_ssg-sle15-xccdf-1.2.xml
        Status: draft
        Generated: 2021-03-24
        Resolved: true
        Profiles:
            Title: CIS SUSE Linux Enterprise 15 Benchmark
                Id: xccdf_org.ssgproject.content_profile_cis
            Title: Standard System Security Profile for SUSE Linux Enterprise 15
                Id: xccdf_org.ssgproject.content_profile_standard
            Title: DISA STIG for SUSE Linux Enterprise 15
                Id: xccdf_org.ssgproject.content_profile_stig
        Referenced check files:
            ssg-sle15-oval.xml
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
            ssg-sle15-ocil.xml
                system: http://scap.nist.gov/schema/ocil/2
            https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15.xml
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
    Ref-Id: scap_org.open-scap_cref_ssg-sle15-oval.xml
    Ref-Id: scap_org.open-scap_cref_ssg-sle15-ocil.xml
    Ref-Id: scap_org.open-scap_cref_ssg-sle15-cpe-oval.xml
Dictionaries:
    Ref-Id: scap_org.open-scap_cref_ssg-sle15-cpe-dictionary.xml
```

记下用于执行扫描的文件路径和配置文件。

20.4.5. 执行审计扫描

安装或传输内容文件后，可以执行审计扫描。可以使用 SUSE Manager Web UI 触发审计扫描。还可以使用 SUSE Manager API 来安排定期扫描。

过程：从 Web UI 运行审计扫描

1. 在 SUSE Manager Web UI 中，导航到**系统 › 系统列表**，然后选择要扫描的客户端。
2. 依次导航到审计选项卡和日程安排子选项卡。
3. 在 `XCCDF 文档的路径`字段中，输入要在客户端上使用的 SCAP 模板和配置文件的参数。例如：

```
命令：/usr/bin/oscap xccdf eval
命令行参数：--profile xccdf_org.ssgproject.content_profile_stig
XCCDF 文档的路径：/usr/share/xml/scap/ssg/content/ssg-sle15-ds-1.2.xml
```

> 如果使用 `--fetch-remote-resources` 参数，将需要大量 RAM。此外，可能还需增加 `file_recv_max_size` 的值。

4. 扫描将在客户端进行下一次安排的同步时运行。

> XCCDF 内容文件在远程系统上运行之前会经过验证。如果内容文件包含无效参数，则测试将会失败。

过程：从 API 运行审计扫描

1. 在开始之前，请确保要扫描的客户端上已安装 Python 和 XML-RPC 库。
2. 选择现有的脚本或创建一个脚本，用于通过 `system.scap.scheduleXccdfScan` 安排系统扫描。例如：

```
#!/usr/bin/python3
client = xmlrpc.client.ServerProxy('https://server.example.com/rpc/api')
key = client.auth.login('username', 'password')
client.system.scap.scheduleXccdfScan(key, <1000010001>,
   '<path_to_xccdf_file.xml>',
   '--profile <profile_name>')
```

   在此示例中： * `<1000010001>` 是系统 ID (sid)。 * `<path_to_xccdf_file.xml>` 是指向客户端上的内容文件位置的路径。例如，`/usr/share/xml/scap/ssg/content/ssg-sle15-ds-1.2.xml`。 * `<profile_name>` 是 `oscap` 命令的附加参数。例如，使用 `united_states_government_configuration_baseline` (USGCB)。

3. 在命令提示符下，对您要扫描的客户端运行该脚本。

20.4.6. 扫描结果

有关已运行的扫描的信息将显示在 SUSE Manager Web UI 中。导航到**审计 › OpenSCAP › 所有扫描**可查看结果表。有关此表中的数据的详细信息，请参见 **Reference › Audit**。

为确保提供有关扫描的详细信息，需要在客户端上启用相应设置。在 SUSE Manager Web UI 中，导航到**管理 › 组织**并单击客户端所在的组织。导航到配置选项卡，并选中启用详细 SCAP 文件上载选项。启用后，每次扫描时都会额外生成一个包含附加信息的 HTML 文件。结果中会显示如下所示的附加行：

```
详细结果：xccdf-report.html xccdf-results.xml scap-yast2sec-oval.xml.result.xml
```

要从命令行检索扫描信息，请使用 `spacewalk-report` 命令：

```
spacewalk-report system-history-scap
spacewalk-report scap-scan
spacewalk-report scap-scan-results
```

还可以使用 SUSE Manager API 通过 `system.scap` 处理程序来查看结果。

20.4.7. 修复

相同 SCAP 安全指南软件包中提供了修复 Bash 脚本和 Ansible 剧本，以强化客户端系统。例如：

列表 6. bash 脚本

```
/usr/share/scap-security-guide/bash/sle15-script-cis.sh
/usr/share/scap-security-guide/bash/sle15-script-standard.sh
/usr/share/scap-security-guide/bash/sle15-script-stig.sh
```

列表 7. Ansible 剧本

```
/usr/share/scap-security-guide/ansible/sle15-playbook-cis.yml
/usr/share/scap-security-guide/ansible/sle15-playbook-standard.yml
/usr/share/scap-security-guide/ansible/sle15-playbook-stig.yml
```

在客户端系统中启用 Ansible 后，可以使用远程命令或 Ansible 运行这些脚本和剧本。

20.4.7.1. 使用 Bash 脚本运行修复

在所有目标系统上安装 `scap-security-guide` 软件包。有关详细信息，请参见 **Administration › Ansible-setup-control-node**。

用于每个操作系统和发行套件的软件包、通道和脚本都不同。修复 Bash 脚本示例 一节中列出了示例。

20.4.7.1.1. 在单个系统上将 Bash 脚本作为远程命令运行

在单个系统上将 Bash 脚本作为远程命令运行。

1. 在**系统 › 概览**选项卡中选择您的实例。然后在**细节 › 远程命令**中编写一个 Bash 脚本，例如：

   ```
   #!/bin/bash
   chmod +x -R /usr/share/scap-security-guide/bash
   /usr/share/scap-security-guide/bash/sle15-script-stig.sh
   ```

2. 单击 **[日程安排]**。

   文件夹和脚本名称在每个发行套件和版本中有差别。修复 Bash 脚本示例 一节列出了示例。

20.4.7.1.2. 在多个系统上使用系统集管理器运行 Bash 脚本

一次性在多个系统上将 Bash 脚本作为远程命令运行。

1. 创建系统组后，单击系统组并从表中选择在 SSM 中使用。
2. 在系统集管理器中的**其他 › 远程命令**下编写一个 Bash 脚本，例如：

   ```
   #!/bin/bash
   chmod +x -R /usr/share/scap-security-guide/bash
   /usr/share/scap-security-guide/bash/sle15-script-stig.sh
   ```

3. 单击 **[日程安排]**。

20.4.7.2. 修复 Bash 脚本示例

20.4.7.2.1. SUSE Linux Enterprise openSUSE 和变体

SUSE Linux Enterprise 和 openSUSE 脚本数据示例。

软件包

scap-security-guide

通道

- SLE12：SLES12 更新
- SLE15：SLES15 模块 Basesystem 更新

Bash 脚本目录

`/usr/share/scap-security-guide/bash/`

Bash 脚本

```
opensuse-script-standard.sh
sle12-script-standard.sh
sle12-script-stig.sh
sle15-script-cis.sh
sle15-script-standard.sh
sle15-script-stig.sh
```

20.4.7.2.2. Red Hat Enterprise Linux 和 CentOS Bash 脚本数据

Red Hat Enterprise Linux 和 CentOS 脚本数据示例。

centos7-updates 中的 `scap-security-guide` 仅包含 Red Hat Enterprise Linux 脚本。

软件包

scap-security-guide-redhat

通道

- SUSE Manager 工具

Bash 脚本目录

`/usr/share/scap-security-guide/bash/`

Bash 脚本

```
centos7-script-pci-dss.sh
centos7-script-standard.sh
centos8-script-pci-dss.sh
centos8-script-standard.sh
fedora-script-ospp.sh
fedora-script-pci-dss.sh
fedora-script-standard.sh
ol7-script-anssi_nt28_enhanced.sh
ol7-script-anssi_nt28_high.sh
```

```
ol7-script-anssi_nt28_intermediary.sh
ol7-script-anssi_nt28_minimal.sh
ol7-script-cjis.sh
ol7-script-cui.sh
ol7-script-e8.sh
ol7-script-hipaa.sh
ol7-script-ospp.sh
ol7-script-pci-dss.sh
ol7-script-sap.sh
ol7-script-standard.sh
ol7-script-stig.sh
ol8-script-anssi_bp28_enhanced.sh
ol8-script-anssi_bp28_high.sh
ol8-script-anssi_bp28_intermediary.sh
ol8-script-anssi_bp28_minimal.sh
ol8-script-cjis.sh
ol8-script-cui.sh
ol8-script-e8.sh
ol8-script-hipaa.sh
ol8-script-ospp.sh
ol8-script-pci-dss.sh
ol8-script-standard.sh
rhel7-script-anssi_nt28_enhanced.sh
rhel7-script-anssi_nt28_high.sh
rhel7-script-anssi_nt28_intermediary.sh
rhel7-script-anssi_nt28_minimal.sh
rhel7-script-C2S.sh
rhel7-script-cis.sh
rhel7-script-cjis.sh
rhel7-script-cui.sh
rhel7-script-e8.sh
rhel7-script-hipaa.sh
rhel7-script-ncp.sh
rhel7-script-ospp.sh
rhel7-script-pci-dss.sh
rhel7-script-rhelh-stig.sh
rhel7-script-rhelh-vpp.sh
rhel7-script-rht-ccp.sh
rhel7-script-standard.sh
rhel7-script-stig_gui.sh
rhel7-script-stig.sh
rhel8-script-anssi_bp28_enhanced.sh
rhel8-script-anssi_bp28_high.sh
rhel8-script-anssi_bp28_intermediary.sh
rhel8-script-anssi_bp28_minimal.sh
rhel8-script-cis.sh
rhel8-script-cjis.sh
rhel8-script-cui.sh
rhel8-script-e8.sh
rhel8-script-hipaa.sh
rhel8-script-ism_o.sh
rhel8-script-ospp.sh
rhel8-script-pci-dss.sh
rhel8-script-rhelh-stig.sh
rhel8-script-rhelh-vpp.sh
rhel8-script-rht-ccp.sh
rhel8-script-standard.sh
rhel8-script-stig_gui.sh
rhel8-script-stig.sh
rhel9-script-pci-dss.sh
rhosp10-script-cui.sh
rhosp10-script-stig.sh
rhosp13-script-stig.sh
rhv4-script-pci-dss.sh
rhv4-script-rhvh-stig.sh
rhv4-script-rhvh-vpp.sh
sl7-script-pci-dss.sh
sl7-script-standard.sh
```

20.4.7.2.3. Ubuntu Bash 脚本数据

Ubuntu 脚本数据示例。

软件包

scap-security-guide-ubuntu

通道

- SUSE Manager 工具

Bash 脚本目录

`/usr/share/scap-security-guide/`

Bash 脚本

```
ubuntu1804-script-anssi_np_nt28_average.sh
ubuntu1804-script-anssi_np_nt28_high.sh
ubuntu1804-script-anssi_np_nt28_minimal.sh
ubuntu1804-script-anssi_np_nt28_restrictive.sh
ubuntu1804-script-cis.sh
ubuntu1804-script-standard.sh
ubuntu2004-script-standard.sh
```

20.4.7.2.4. Debian Bash 脚本数据

Debian 脚本数据示例。

软件包

scap-security-guide-debian

通道

- SUSE Manager 工具

Bash 脚本目录

`/usr/share/scap-security-guide/bash/`

Bash 脚本

```
debian10-script-anssi_np_nt28_average.sh
debian10-script-anssi_np_nt28_high.sh
debian10-script-anssi_np_nt28_minimal.sh
debian10-script-anssi_np_nt28_restrictive.sh
debian10-script-standard.sh
debian11-script-anssi_np_nt28_average.sh
debian11-script-anssi_np_nt28_high.sh
debian11-script-anssi_np_nt28_minimal.sh
debian11-script-anssi_np_nt28_restrictive.sh
debian11-script-standard.sh
```

20.5. 审计

在 SUSE Manager 中，您可以通过一系列审计任务来跟踪客户端。您可以检查客户端上是否安装了所有最新的

公共安全补丁 (CVE)，执行订阅匹配，并使用 OpenSCAP 检查合规性。

在 SUSE Manager Web UI 中，导航到审计执行审计任务。

20.5.1. CVE 审计

CVE（公共漏洞和暴露）是对众所周知的安全漏洞的修复。

> 只要有可用的 CVE，就必须在客户端上应用它们。

每个 CVE 包含一个标识号、漏洞说明以及更多信息的链接。CVE 标识号使用 `CVE-YEAR-XXXX` 格式。

在 SUSE Manager Web UI 中，导航到**审计 › CVE 审计** 以查看所有客户端及其当前补丁状态的列表。

默认情况下，CVE 数据在每天 23:00 更新。我们建议您在开始进行 CVE 审计之前刷新数据，以确保应用最新的补丁。

程序：更新 CVE 数据

1. 在 SUSE Manager Web UI 中，导航到**管理 › 任务日程安排**，然后选择 `cve-server-channels-default` 日程安排。
2. 单击 **[cve-server-channels-bunch]**。
3. 单击 **[单次运行安排]** 以安排任务。 等待该任务完成，然后继续进行 CVE 审计。

过程：校验补丁状态

1. 在 SUSE Manager Web UI 中，导航到**审计 › CVE 审计**。
2. 要检查特定 CVE 的补丁状态，请在 `CVE 编号`字段中键入 CVE 标识符。
3. 选择您要查看的补丁状态，或保持选中所有状态以查看所有补丁状态。
4. 单击 **[审计服务器]** 检查所有系统，或单击 **[审计映像]** 检查所有映像。

有关此页面上使用的补丁状态图标的详细信息，请参见 **Reference › Audit**。

对于每个系统，下一个操作列会提供有关需要采取哪些措施才能解决漏洞的信息。如果适用，其中还会列出候选通道或补丁。您还可以将系统指派到系统集以做进一步的批处理。

可以使用 SUSE Manager API 来校验客户端的补丁状态。使用 `audit.listSystemsByPatchStatus` API 方法。有关此方法的详细信息，请参见《SUSE Manager API 指南》。

20.5.2. CVE 状态

客户端的 CVE 状态通常是受影响、不受影响或已增补。这些状态仅取决于 SUSE Manager 适用的信息。

在 SUSE Manager 中，以下定义适用：

受特定漏洞影响的系统

系统中安装的某个软件包版本低于标记为漏洞的相关补丁中相同软件包的版本。

不受特定漏洞影响的系统

同时包含在标记为漏洞的相关补丁中的软件包未安装在系统上。

针对某个漏洞进行了增补的系统

系统中安装的某个软件包版本等同于或高于标记为漏洞的相关补丁中相同软件包的版本。

相关补丁

SUSE Manager 在相关通道中已知的补丁。

相关通道

由 SUSE Manager 管理的通道，该通道被指派到系统、是指派到系统的克隆通道的原始通道、是链接到系统上安装的产品的通道，或者是系统的过去或将来的服务包通道。

由于 SUSE Manager 中使用的定义，CVE 审计结果在某些情况下可能不正确。例如，非受管通道、非受管软件包或不合规的系统可能会错误地报告结果。

Chapter 21. SSL 证书

SUSE Manager 使用 SSL 证书来确保客户端注册到正确的服务器。

每个使用 SSL 注册到 SUSE Manager Server 的客户端将通过验证服务器证书来检查它是否连接到正确的服务器。此过程称为 SSL 握手。

在 SSL 握手期间，客户端将检查服务器证书中的主机名是否与预期相符。客户端还需要检查服务器证书是否受信任。

证书颁发机构 (CA) 是用于为其他证书签名的证书。所有证书必须由证书颁发机构 (CA) 签名，只有这样，才会将它们视为有效，并且客户端才能成功地匹配它们。

为使 SSL 身份验证能够正常进行，客户端必须信任根 CA。这意味着必须在每个客户端上安装根 CA。

默认的 SSL 身份验证方法是让 SUSE Manager 使用自我签名证书。在这种情况下，SUSE Manager 已生成所有证书，并且根 CA 已直接为服务器证书签名。

另一种方法是使用中间 CA。在这种情况下，根 CA 为中间 CA 签名。然后中间 CA 可为任意数量的其他中间 CA 签名，而最后一个中间 CA 为服务器证书签名。这称为链式证书。

如果您在链式证书中使用中间 CA，则根 CA 将安装在客户端上，而服务器证书则安装在服务器上。在 SSL 握手期间，客户端必须能够校验根 CA 与服务器证书之间的整个中间证书链，因此它们必须能够访问所有中间证书。

可以通过两种主要方式实现此目的。在较旧版本的 SUSE Manager 中，所有中间 CA 默认都安装在客户端上。但是，您也可以在服务器上配置服务以将其提供给客户端。在这种情况下，在 SSL 握手期间，服务器会提供服务器证书以及所有中间 CA。此机制现已用作新的默认配置。

SUSE Manager 默认使用没有中间 CA 的自我签名证书。为了提高安全性，您可以安排一个第三方 CA 来为您的证书签名。第三方 CA 执行检查以确保证书中包含的信息正确。他们通常针对此项服务收取年费。使用第三方 CA 可以提高证书的伪造难度，并为安装提供附加的保护。如果您的证书已由第三方 CA 签名，您可以将其导入 SUSE Manager 安装中。

本手册分 2 个步骤介绍 SSL 证书的用法

1. 如何使用 SUSE Manager 工具创建自我签名证书
2. 如何在 SUSE Manager Server 或 Proxy 上部署证书

如果证书由第三方实例（例如自有或外部的 PKI）提供，则可以跳过步骤 1。

- 有关如何创建自我签名证书的详细信息，请参见 **Administration › Ssl-certs-selfsigned**。
- 有关如何导入证书的详细信息，请参见 **Administration › Ssl-certs-imported**。

21.1. 自我签名 SSL 证书

SUSE Manager 默认使用自我签名证书。在这种情况下，证书由 SUSE Manager 创建和签名。此方法不使用独

立证书颁发机构来保证证书的细节正确。第三方 CA 将执行检查，以确保证书中包含的信息正确。有关第三方 CA 的详细信息，请参见 **Administration › Ssl-certs-imported**。

本节介绍如何在新安装或现有安装中创建或重新创建自我签名证书。

SSL 密钥和证书的主机名必须与其部署到的计算机的完全限定主机名相匹配。

21.1.1. 重新创建现有的服务器证书

如果您的现有证书已失效或出于任何原因而不再正常工作，您可以从现有 CA 生成新的服务器证书。

过程：重新创建现有服务器证书

1. 在 SUSE Manager Server 上的命令提示符下，重新生成服务器证书：

```
rhn-ssl-tool --gen-server --dir="/root/ssl-build" --set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname="susemanager.example.com" --set-cname="example.com"
```

   确保 `set-cname` 参数是您的 SUSE Manager Server 的完全限定域名。如果需要多个别名，可以多次使用 `set-cname` 参数。

私用密钥和服务器证书可以在目录 `/root/ssl-build/susemanager/` 中找到，其文件名为 `server.key` 和 `server.crt`。最后一个目录的名称取决于与 `--set-hostname` 选项结合使用的主机名。

21.1.2. 创建新的 CA 证书和服务器证书

> 替换根 CA 时请小心。这可能会破坏服务器与客户端之间的信任链。如果发生这种情况，需要让某个管理用户登录到每个客户端并直接部署 CA。

过程：创建新证书

1. 在 SUSE Manager Server 上的命令提示符下，将旧证书目录移到新位置：

```
mv /root/ssl-build /root/old-ssl-build
```

2. 生成新的 CA 证书：

```
rhn-ssl-tool --gen-ca --dir="/root/ssl-build" --set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-common-name="SUSE Manager CA Certificate" \
--set-email="name@example.com"
```

3. 生成新的服务器证书：

```
rhn-ssl-tool --gen-server --dir="/root/ssl-build" --set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname="susemanager.example.top" --set-cname="example.com"
```

确保 `set-cname` 参数是您的 SUSE Manager Server 的完全限定域名。如果需要多个别名，可以多次使用 `set-cname` 参数。

还需要使用代理的主机名和 cname 为每个代理生成一个服务器证书。

21.2. 导入 SSL 证书

本节介绍如何为新的 SUSE Manager 安装配置 SSL 证书，以及如何替换现有证书。

在开始之前，请确保已准备好：

- 一个证书颁发机构 (CA) SSL 公共证书。如果您使用 CA 链，则所有中间 CA 也必须可用。
- 一个 SSL 服务器私用密钥
- 一个 SSL 服务器证书

所有文件必须采用 PEM 格式。

SSL 服务器证书的主机名必须与其部署到的计算机的完全限定主机名匹配。可以在证书的 `X509v3 Subject Alternative Name` 部分中设置主机名。还可以根据环境的需要列出多个主机名。支持的密钥类型为 `RSA` 和 `EC`（椭圆曲线）。

第三方颁发机构通常使用中间 CA 来为请求的服务器证书签名。在这种情况下，链中的所有 CA 都必须可用。如果没有额外的参数或选项可用于指定中间 CA，请注意所有 CA（根 CA 和中间 CA）都将存储在一个文件中。

21.2.1. 为新安装导入证书

SUSE Manager 默认使用自我签名证书。完成初始设置后，可将默认证书替换为导入的证书。

过程：在新的 SUSE Manager Server 上导入证书

1. 根据 **Installation-and-upgrade › Install-intro** 中的说明安装 SUSE Manager Server。
2. 根据 **Installation-and-upgrade › Server-setup** 完成初始设置。
3. 在命令提示符下，将 SSL 环境变量指向证书文件位置：

```
export CA_CERT=<CA 证书文件的路径>
export SERVER_KEY=<Web 服务器密钥的路径>
export SERVER_CERT=<Web 服务器证书的路径>
```

4. 完成 SUSE Manager 设置：

```
yast susemanager_setup
```

在设置过程中，当系统提示您输入证书细节时，请填写随机值。这些值将由您在命令提示符下指定的值覆盖。

> 在从中导出了环境变量的同一个外壳中执行 `yast susemanager_setup` 命令。

21.2.2. 为新的 Proxy 安装导入证书

SUSE Manager Proxy 默认使用自我签名证书。完成初始设置后，您可以将默认证书替换为导入的证书。

过程：在新的 SUSE Manager Proxy 上导入证书

1. 根据**Installation-and-upgrade › Install-intro**中的说明安装 SUSE Manager Proxy。
2. 根据**Installation-and-upgrade › Proxy-setup**完成初始设置。
3. 在命令提示符下，运行：

```
configure-proxy.sh
```

4. 出现您要导入现有证书吗？提示时，键入 `y`。
5. 按照提示完成设置。

> 使用同一证书颁发机构为服务器和代理的所有服务器证书签名。使用不同 CA 签名的证书将不匹配。

21.2.3. 替换证书

您可以将 SUSE Manager 安装中的活动证书替换为新证书。要替换证书，可以将已安装的 CA 证书替换为新 CA，然后更新数据库。

过程：替换现有证书

1. 在 SUSE Manager Server 上的命令提示符下，调用命令 `mgr-ssl-cert-setup` 并提供证书作为参数：

```
mgr-ssl-cert-setup --root-ca-file=<根 CA 证书的路径> --server-cert-file=<服务器证书文件>
--server-key-file=<服务器密钥文件>
```

中间 CA 可以在使用 `--root-ca-file` 指定的文件中提供，也可以使用 `--intermediate-ca-file` 作为附加选项来指定。可以多次指定 `--intermediate-ca-file` 选项。此命令将对提供的文件执行一些测试，以测试它们是否有效并可用于请求的用例。

1. 重启动服务以应用更改：

```
spacewalk-service stop
systemctl restart postgresql.service
spacewalk-service start
```

如果您使用代理，则需要使用代理的主机名和 cname 为每个代理生成一个服务器证书 RPM。还应在 SUSE Manager 代理上使用 `mgr-ssl-cert-setup` 来替换证书。由于 SUSE Manager 代理没有 postgreSQL 数据库，因此运行 `spacewalk-service restart` 就已足够。

如果根 CA 已更改，则需要将其部署到与 SUSE Manager 连接的所有客户端。

过程：在 Salt 客户端上部署根 CA

1. 在 SUSE Manager Web UI 中，导航到**系统 › 概览**。
2. 选中所有 Salt 客户端以将其添加到系统集管理器。
3. 导航到**系统 › 系统集管理器 › 概览**。
4. 在状态字段中，单击 **[应用]** 以应用系统状态。
5. 在 `Highstate` 页面中，单击 **[应用 Highstate]** 以将更改传播到客户端。

21.2.3.1. 传统客户端的额外处理

传统客户端已弃用，请改用 Salt 客户端。

在仍有传统受管客户端连接到 SUSE Manager 的情况下，如果需要替换 CA，则需要执行一些额外的步骤。

重要的是，当新 CA 在 SUSE Manager Server 和 Proxy 上激活时，这些客户端不会断开连接。将旧的和新的根 CA 证书部署到受影响的客户端并信任这些证书。使用配置通道将证书文件部署到客户端，并使用远程命令功能重新生成信任存储。

在 SUSE Manager Server 和 Proxy 上激活新证书后，测试连接是否正常，以及是否仍然可以在客户端上安排操作。如果一切正常，则可以从客户端中去除旧的根 CA。

21.3. HTTP 严格传输安全性

HTTP 严格传输安全性 (HSTS) 是帮助防范网站遭受中间人攻击（例如协议降级攻击和 Cookie 劫持）的策略机制。

SUSE Manager 允许启用 HSTS。要为 SUSE Manager Server 启用 HSTS，请执行以下操作：

过程

1. 在 `/etc/apache2/conf.d/<filename>.conf` 中创建新配置文件，例如 `/etc/apache2/conf.d/zz-spacewalk-www-custom.conf`。
2. 添加以下一行：`# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"`
3. 使用 `systemctl restart apache2` 重启动 Apache

要为 SUSE Manager Proxy 启用 HSTS，请执行以下操作：

过程

1. 在 `/etc/apache2/conf.d/<filename>.conf` 中创建新配置文件，例如 `/etc/apache2/conf.dz/zz-spacewalk-proxy-custom.conf`。
2. 添加以下一行：`# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"`
3. 使用 `systemctl restart apache2` 重启动 Apache

为新配置文件 `<filename>.conf` 命名时，请确保它能在正确的时间加载。例如，要覆盖 `spacewalk-www.conf` 中定义的某些设置，新文件需位于此文件之后（按字母顺序）。有关 Apache 如何加载文件的详细信息，请参见 https://httpd.apache.org/docs。

在使用 SUSE Manager 生成的默认 SSL 证书或自我签名证书的情况下启用 HSTS 后，浏览器将拒绝通过 HTTPS 进行连接，除非用于为此类证书签名的 CA 受浏览器信任。如果您使用的是 SUSE Manager 生成的 SSL 证书，可以通过将 http://<服务器主机名>/pub/RHN-ORG-TRUSTED-SSL-CERT 中的文件导入到所有用户的浏览器来信任该证书。

Chapter 22. 订阅匹配

您的 SUSE 产品需要订阅，订阅由 SUSE Customer Center (SCC) 管理。SUSE Manager 会运行夜间报告，以检查您的 SCC 帐户的所有已注册客户端的订阅状态。该报告提供有关哪些客户端使用哪些订阅、您的剩余订阅数和可用订阅数，以及哪些客户端没有当前订阅的信息。

导航到**审计 › 订阅匹配**以查看报告。

订阅报告选项卡提供有关当前订阅和即将失效的订阅的信息。

不匹配的产品报告选项卡提供没有当前订阅的客户端列表。这包括无法匹配的客户端，或当前未注册到 SUSE Manager 的客户端。该报告包括产品名称和不匹配的系统数。

在关联选项卡中，可以将各个客户端关联到相关的订阅。如果订阅管理器无法成功地将客户端自动关联到订阅，此选项卡特别有用。

消息索引标签显示订阅匹配器在匹配过程中生成的所有消息。这些消息提供有助于用户了解结果和改进匹配的信息。

您还可以下载 .csv 格式的报告，或者从命令提示符在 `/var/lib/spacewalk/subscription-matcher/` 目录中访问这些报告。

默认情况下，订阅匹配器每日午夜运行。要更改此设置，请导航到**管理 › 任务日程安排**并单击 `gatherer-matcher-default`。根据需要更改日程安排，然后单击 **[更新日程安排]**。

由于报告只能将当前客户端与当前订阅相匹配，因此您可能会发现匹配结果随时间而变化。同一个客户端不一定总与同一个订阅匹配。原因可能是新客户端正在注册或未注册，或者添加了订阅或订阅失效。

订阅匹配器会自动尝试减少不匹配的产品数量，具体数量受您帐户中订阅的条款和条件限制。但是，如果硬件信息不完整、虚拟机主机指派未知，或者客户端在未知公有云中运行，则匹配器可能会显示您没有足够的可用订阅。请务必提供有关 SUSE Manager 中您的客户端的完整数据，以帮助确保信息准确。

> 订阅匹配器不一定总能准确匹配客户端和订阅。它并非旨在替代审计功能。

22.1. 将客户端关联到订阅

如果订阅匹配器无法自动将特定客户端与正确的订阅相匹配，您可以手动关联它们。创建关联后，订阅匹配器倾向于将特定订阅与给定的系统或系统组相匹配。

但是，匹配器并非始终遵守关联。这取决于订阅是否可用，以及订阅是否可以应用于该客户端。此外，如果关联导致匹配违反订阅的条款和条件，或者如果匹配器检测到在忽略关联的情况下匹配结果更准确，则就会忽略关联。

要添加新关联，请单击 **[添加关联]**，然后选择要关联的客户端。

我们不建议经常性使用关联或者对大量客户端使用关联。对于大多数安装而言，订阅匹配器工具通常已足够准确。

Chapter 23. 任务日程安排

管理 › 任务日程安排下会列出所有预定义的任务组。

SUSE Manager Schedules

+ create schedule

Below is a list of defined schedules. A schedule defines frequency, how often a predefined bunch shall be triggered.

1 - 23 of 23

25 items per page

Schedule name	Frequency	Active From	Bunch
auto-errata-default	0 5/10 * * * ?	2018-06-05 11:40:50 CEST	auto-errata-bunch
channel-repodata-default	0 * * * * ?	2018-06-05 11:40:50 CEST	channel-repodata-bunch
cleanup-data-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	cleanup-data-bunch
clear-taskologs-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	clear-taskologs-bunch
cobbler-sync-default	0 * * * * ?	2018-06-05 11:40:50 CEST	cobbler-sync-bunch
compare-configs-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	compare-configs-bunch
cve-server-channels-default	0 0 23 ? * *	2018-06-05 11:40:51 CEST	cve-server-channels-bunch
daily-status-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	daily-status-bunch
errata-cache-default	0 * * * * ?	2018-06-05 11:40:50 CEST	errata-cache-bunch
errata-queue-default	0 * * * * ?	2018-06-05 11:40:50 CEST	errata-queue-bunch
gatherer-matcher-default	0 0 0 ? * *	2018-06-05 11:40:51 CEST	gatherer-matcher-bunch
kickstart-cleanup-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	kickstart-cleanup-bunch
kickstartfile-sync-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	kickstartfile-sync-bunch
mgr-register-default	0 0/15 * * * ?	2018-06-05 11:40:50 CEST	mgr-register-bunch
mgr-sync-refresh-default	0 6 1 ? * *	2018-06-05 11:40:51 CEST	mgr-sync-refresh-bunch
minion-action-cleanup-default	0 0 * * * ?	2018-06-05 11:40:50 CEST	minion-action-cleanup-bunch
package-cleanup-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	package-cleanup-bunch
reboot-action-cleanup-default	0 0 * * * ?	2018-06-05 11:40:50 CEST	reboot-action-cleanup-bunch
sandbox-cleanup-default	0 5 4 ? * *	2018-06-05 11:40:50 CEST	sandbox-cleanup-bunch
session-cleanup-default	0 0/15 * * * ?	2018-06-05 11:40:50 CEST	session-cleanup-bunch
ssh-push-default	0 * * * * ?	2018-06-05 11:40:50 CEST	ssh-push-bunch
token-cleanup-default	0 0 0 ? * *	2018-06-05 11:40:51 CEST	token-cleanup-bunch
uuid-cleanup-default	0 0 * * * ?	2018-06-05 11:40:51 CEST	uuid-cleanup-bunch

单击 **SUSE Manager 日程安排 › 日程安排名称**可打开**日程安排名称 › 日程安排基本细节**，在其中可以禁用该日程安排或更改频率。

单击 **[编辑日程安排]** 可使用您的设置更新该日程安排。

要删除日程安排，请单击右上角的 **[删除日程安排]**。

请仅在绝对有必要的情况下才禁用或删除日程安排，因为日程安排对于 SUSE Manager 正常运行至关重要。

如果您单击某个组名称，将显示该组类型的运行列表和运行状态。

单击开始时间链接会返回**日程安排名称 › 日程安排基本细节**。

23.1. 预定义的任务组

系统默认会安排以下预定义的任务组，您可对其进行配置：

auto-errata-default

根据需要安排自动勘误更新。

channel-repodata-default

（重新）生成储存库元数据文件。

cleanup-data-default

从数据库中清理已过时的软件包更改日志和监视时序数据。

clear-taskologs-default

根据作业类型，从数据库中清除超过指定天数的任务引擎 (taskomatic) 历史数据。

cobbler-sync-default

将 SUSE Manager 中的分布数据和配置文件数据同步到 Cobbler。有关由 Cobbler 提供支持的自动安装的详细信息，请参见 **Client-configuration › Autoinst-intro**。

compare-configs-default

将存储在配置通道中的配置文件与存储在所有已启用配置的服务器上的文件进行比较。要查看比较结果，请单击**系统**选项卡并选择相关系统。转到**配置 › 比较文件**。有关详细信息，请参见 reference:systems/system-details/sd-configuration.pdf。

cve-server-channels-default

更新用于在**审计 › CVE 审计**页面上显示结果的内部预计算 CVE 数据。**审计 › CVE 审计**页面中的搜索结果将根据此日程安排的上次运行情况更新。有关详细信息，请参见 **Reference › Audit**。

daily-status-default

将每日报告电子邮件发送到相关地址。有关如何为特定用户配置通知的详细信息，请参见 **Reference › Users**。

errata-cache-default

更新内部补丁缓存数据库表，这些表用于查找每个服务器的需要更新的软件包。此任务组还向可能对特定补丁感兴趣的用户发送通知电子邮件。有关补丁的详细信息，请参见 **Reference › Patches**。

errata-queue-default

为配置为接收自动更新（补丁）的服务器将这些更新（补丁）排队。

gatherer-matcher-default

通过运行在虚拟主机管理器中配置的虚拟主机收集器，来收集虚拟主机数据。当有更新的数据后，订阅匹配器作业即会运行。

kickstart-cleanup-default

清理过时的 Kickstart 会话数据。

kickstartfile-sync-default

生成与配置向导创建的 Kickstart 配置文件对应的 Cobbler 文件。

mgr-forward-registration-default

将客户端注册数据与 SUSE Customer Center 同步。默认会转发新的、已更改的或已删除的客户端数据。要禁用 `/etc/rhn/rhn.conf` 中设置的同步，请运行：

```
server.susemanager.forward_registration = 0
```

> Disabling data synchronizing with SCC will lead to reduced visibility of your managed clients between RMT, SMT, SUSE Manager and SCC-directly registered clients. By synchronizing data, you ensure a uniform view of all registered clients. Help us improve our services by sharing your reason for opting out

mgr-sync-refresh-default

与 SUSE Customer Center 保持同步 (`mgr-sync-refresh`)。默认情况下，在此任务执行过程中也会同步所有自定义通道。有关自定义通道同步的详细信息，请参见 administration:custom-channels.pdf。

minion-action-chain-cleanup-default

清理过时的操作链数据。

minion-action-cleanup-defaul:

从文件系统中删除过时的客户端操作数据。首先，此任务组会尝试通过查找存储在 Salt 作业缓存中的相应结果，来完成任何可能未完成的操作。如果服务器遗漏了操作结果，就可能发生操作未完成的情况。对于成功完成的操作，此任务组会去除已执行的脚本文件等项目。

minion-checkin-default

在客户端上执行常规的签入。

notifications-cleanup-default

清理失效的通知消息。

package-cleanup-default

从文件系统中删除过时的软件包文件。

reboot-action-cleanup-default

任何超过六个小时未处理的重引导操作都将标记为失败，数据库中的关联数据将被清理。有关安排重引导操作的详细信息，请参见 reference:systems/system-details/sd-provisioning.pdf。

sandbox-cleanup-default

清理超过 sandbox_lifetime 配置参数值（默认值为 3 天）的沙箱配置文件和通道。沙箱文件是从系统导入的文件或正在开发的文件。有关详细信息，请参见 reference:systems/system-details/sd-

configuration.pdf。

session-cleanup-default

清理过时的 Web 界面会话，这通常是用户登录之后，在注销之前关闭浏览器时临时存储的数据。

ssh-push-default

如果为客户端配置了 `SSH Push` 联系方法，则提示客户端通过 SSH 来与 SUSE Manager 通讯。

system-profile-refresh-default

在所有系统上执行硬件刷新。此任务组每月只执行一次，可能会增加 SUSE Manager 服务器上的负荷。该作业会使用 **Specialized-guides** › **Salt**。如果要调整批次大小，请参见 specialized-guides:large-deployments/tuning.pdf。

token-cleanup-default

删除 Salt 客户端用来下载软件包和元数据的已失效储存库令牌。

update-payg-default

从配置的 PAYG 云实例收集身份验证数据。

update-reporting-default

更新本地报告数据库。

update-reporting-hub-default

从外围 SUSE Manager 服务器收集所有报告数据，并更新 Hub Reporting 数据库。

uuid-cleanup-default

清理过时的 UUID 记录。

Chapter 24. 微调更改日志

某些软件包的更改日志项列表很长。默认会下载这些数据，但日志中保留的信息不一定有用。为了限制下载的更改日志元数据量并节省磁盘空间，您可以对磁盘上保留的项数施加限制。

此配置选项保存在 `/etc/rhn/rhn.conf` 配置文件中。该参数默认设置为 `20`；将此值更改为 `0` 将提供不限数量的项。

```
java.max_changelog_entries = 20
```

如果您设置此参数，它只在同步新软件包后对其生效。

更改此参数后，请使用 `spacewalk-service restart` 重启动服务。

您可能想要删除再重新生成缓存的数据，以去除旧数据。

> 删除再重新生成缓存的数据可能需要很长时间。根据您的通道数量和要删除的数据量，此过程可能需要几个小时。该任务由 Taskomatic 在后台运行，因此您可以在操作完成时继续使用 SUSE Manager，但应该预料到性能会有所下降。

可以从命令行删除缓存的数据并请求重新生成数据：

```
spacewalk-sql -i
```

然后在 SQL 数据库提示符下输入：

```
DELETE FROM rhnPackageRepodata;
INSERT INTO rhnRepoRegenQueue (id, CHANNEL_LABEL, REASON, FORCE)
(SELECT sequence_nextval('rhn_repo_regen_queue_id_seq'),
      C.label,
      'cached data regeneration',
      'Y'
      FROM rhnChannel C);
\q
```

Chapter 25. 用户

SUSE Manager 管理员可以添加新用户、授予权限以及停用或删除用户。如果您正在管理大量的用户，可以将用户指派到系统组，以便在组级别管理权限。还可以更改 Web UI 的系统默认值，包括语言和主题默认值。

仅当您使用 SUSE Manager 管理员帐户登录时，用户菜单才可用。

要管理 SUSE Manager 用户，请导航到**用户 › 用户列表 › 所有**以查看 SUSE Manager Server 中的所有用户。列表中的每个用户会显示用户名、真实姓名、指派的角色、用户上次登录日期，以及用户的当前状态。单击**[创建用户]**可以创建新的用户帐户。单击用户名会进入用户细节页面。

要将新用户添加到您的组织，请单击 **[创建用户]**，填写新用户的细节，然后单击 **[创建登录名]**。

25.1. 停用和删除帐户

您可以停用或删除不再需要的用户帐户。已停用的用户帐户随时可以重新激活。已删除的用户帐户将不可见，且不可检索。

用户可以停用自己的帐户。但是，如果用户具有管理员角色，则必须先去除该角色，然后才能停用帐户。

已停用的用户无法登录到 SUSE Manager Web UI 或安排任何操作。用户在停用之前安排的操作将保留在操作队列中。SUSE Manager 管理员可以重新激活已停用的用户。

25.2. 管理员角色

用户可以充当多个管理员角色，并且在任何时候都可以有多个用户充当任一管理员角色。必须始终有至少一名处于活动状态的 SUSE Manager 管理员。

要更改用户的管理员角色（SUSE Manager 管理员角色除外），请导航到**用户 › 用户列表 › 所有**，选择要更改的用户，然后根据需要选中或取消选中管理员角色。

要更改用户的 SUSE Manager 管理员角色，请导航到**管理 › 用户**，并根据需要选中或取消选中 `SUSE Manager Admin?` 。

表格 13. 用户管理员角色权限

角色名称	说明
系统组用户	与所有用户关联的标准角色。
SUSE Manager 管理员	可以执行所有功能，包括更改其他用户的特权。
组织管理员	管理激活密钥、配置、通道和系统组。
激活密钥管理员	管理激活密钥。
映像管理员	管理映像配置文件、构建和存储区。

角色名称	说明
配置管理员	管理系统配置。
通道管理员	管理软件通道，包括使通道全局可订阅，以及创建新通道。
系统组管理员	管理系统组，包括创建和删除系统组、将客户端添加到现有组，以及管理用户对组的访问权限。

25.3. 用户权限和系统

如果您已创建系统组来管理客户端，可以将组指派到用户，让他们进行管理。

要将用户指派到系统组，请导航到**用户 › 用户列表**，单击要编辑的用户名，然后转到系统组选项卡。选中要指派的组，然后单击 **[更新默认值]**。

您还可以为用户选择一个或多个默认系统组。当该用户注册新客户端时，默认会将其指派到所选的系统组。这样，该用户就能立即访问新注册的客户端。

要管理外部组，请导航到**用户 › 系统组配置**，然后转到外部身份验证选项卡。单击 **[创建外部组]** 以创建一个新的外部组。为该组命名，并将其指派到适当的系统组。

有关系统组的详细信息，请参见 **Reference › Systems**。

要查看用户可以管理的各个客户端，请导航到**用户 › 用户列表**，单击要编辑的用户名，然后转到系统选项卡。要执行批量任务，可以从列表中选择客户端以将其添加到系统集管理器。

有关系统集管理器的详细信息，请参见 **Client-configuration › System-set-manager**。

25.4. 用户和通道权限

可以将用户作为使用通道内容的订阅者，或者作为可以自行管理通道的管理员，指派到组织中的软件通道。

要为用户订阅通道，请导航到**用户 › 用户列表**，单击要编辑的用户名，然后转到**通道权限 › 订阅**选项卡。选中要指派的通道，然后单击 **[更新权限]**。

要为用户授予通道管理权限，请导航到**用户 › 用户列表**，单击要编辑的用户名，然后转到**通道权限 › 管理**选项卡。选中要指派的通道，然后单击 **[更新权限]**。

列表中的某些通道可能无法订阅。原因通常与用户的管理员状态或通道全局设置有关。

25.5. 用户默认语言

创建新用户时，您可以选择 Web UI 使用的语言。创建用户后，可以通过导航到**首页 › 我的首选项**来更改语言。

默认语言是在 `rhn.conf` 配置文件中设置的。要更改默认语言，请打开 `/etc/rhn/rhn.conf` 文件并添加或编辑下

面一行内容：

```
web.locale = <语言代码>
```

如果未设置该参数，则默认语言为 `en_US`。

在 SUSE Manager 中可以使用以下语言：

表格 14. 可用语言代码

语言代码	语言	方言
`en_US`	英语	美国
`zh_CN`	中文	中国大陆简体

25.5.1. 用户默认界面主题

SUSE Manager Web UI 默认使用适用于您所安装的产品的主题。您可以更改主题以反映 Uyuni 或 SUSE Manager 颜色。SUSE Manager 主题还提供深色选项。

您可以在 `rhn.conf` 配置文件中更改默认主题。要更改默认主题，请打开 `/etc/rhn/rhn.conf` 文件并添加或编辑下面一行内容：

```
web.theme_default = <主题>
```

表格 15. 可用的 WebUI 主题

主题名称	颜色	样式
`susemanager-light`	SUSE Manager	浅色
`susemanager-dark`	SUSE Manager	深色
`uyuni`	Uyuni	浅色

Chapter 26. 在 SUSE Manager 中使用 PTF

SUSE 为目前支持的所有解决方案提供直接交付给客户的临时修复。这些 PTF（程序临时修复）现在以储存库的形式提供，后者可在 SUSE Manager 中同步。

26.1. 了解 PTF 软件包

PTF 软件包通过代理软件包安装，命名为 `ptf-xxxxxx`。其中 xxxxxx 是软件包的编号和名称部分，而不是版本。

它们取决于已知包含软件中的修正的软件包正确版本。这种软件包：

- 不可能意外安装（即 zypper 更新绝不会建议安装它们），
- 不可能意外去除（即更新的软件包版本不会替换 PTF 软件包，除非用户在 zypper 命令行上明确指示替换），
- 仅会在已知有更新版本可解决该 PTF 之前所解决的特定问题时更新，
- 仅会在系统上已安装软件包时更新（也就是说，如果软件拆分成多个软件包，该 PTF 仅会替换系统上目前安装的那些软件包）。

软件包的正确 ID 将由 SUSE 支持团队在进行支持案例调查期间提供，同时还会提供有关如何部署/重启动受影响服务的说明。

26.2. 安装 PTF 软件包

> PTF 软件包目前仅受基于 SLE 12 和 SLE 15 的系统支持。其他版本或操作系统尚不提供此功能，因此未显示与其对应的页面。

过程：使用命令行启用和同步 PTF 储存库

1. 在控制台上输入 `mgr-sync refresh`。
2. 输入 `mgr-sync list channel`，然后查找以您的 SCC 帐户名称开头且名称中包含 `ptfs` 的通道。例如 `a123456-sles-15.3-ptfs-x86_64`。
3. 使用 `mgr-sync add channel <标签>` 启用该 PTF 通道。

此通道现在便可供使用，并可添加到使用相同基础通道的每个系统。

您需要明确安装 PTF 软件包，因为在更新系统时它们不会自动被选中。SUSE 客户支持团队将提供用于修复特定问题的 PTF 编号。可以使用该编号在 PTF 列表中标识该代理软件包。SUSE Manager Web UI 中会针对有可供安装的 PTF 的每个系统显示一个页面来列出这些 PTF。

过程：通过 SUSE Manager Web UI 启用和同步 PTF 储存库

1. 在 SUSE Manager Web UI 中，导航到**管理 › 安装向导 › 产品**，然后查找要为其启用 PTF 储存库的产品。
2. 单击产品同步状态旁边的 **[显示产品的通道]**。

3. 您应该会看到一个弹出窗口，其中会列出该产品的必需和可选通道。
4. 在可选通道列表中，查找以您的 SCC 帐户名称开头且名称中包含 `ptfs` 的通道。例如 `a123456-sles-15.3-ptfs-x86_64`。
5. 使用该通道名称旁边的复选框将其选中，然后单击 **[确认]** 安排同步。

请注意，必须安装该产品才能为其添加可选通道。

过程：安装 PTF 软件包

1. 在 SUSE Manager Web UI 中，导航到**系统 › 系统列表**，然后选择要安装 PTF 的客户端。
2. 导航到**系统 › 软件 › 软件包 › 软件通道**，然后选择 PTF 通道。
3. 单击 **[下一步]**，然后单击 **[确认]** 以确认软件通道更改。
4. 导航到**系统 › 事件 › 历史记录**查看结果，确定是否已完成通道指派。
5. 导航到**系统 › 软件 › PTF › 安装**子选项卡。
6. 选择要安装的 PTF 软件包。
7. 单击 **[安装 PTF]**，然后单击 **[确认]** 以确认安装程序临时修复（PTF）。
8. 导航到**系统 › 事件 › 历史记录**查看 PTF 安装结果。

如果应使用 API 安装 PTF，可以使用常规 `system.schedulePackageInstall` API 和代理软件包名称。

26.3. 安装 PTF 后

一旦确认使用某个 PTF 来解决报告的问题，在将更新的软件包作为更新储存库中的常规维护更新广泛分发之前，需对其进行跟踪，以便在将来的维护更新中纳入该软件包。

在发布包含修复的此常规更新时，还会将 PTF 的一个更新版本发布到特定于帐户的 PTF 储存库中。更新的 PTF 将会解除严格的依赖关系，并允许再次安装更新。

通过标准软件包更新或补丁安装可自动将 PTF 替换为包含该修复的维护更新。

26.4. 去除软件包的已修补版本

如果需要在系统上卸装某个 PTF 并安装软件包的未修补版本，仅执行软件包去除流程无法实现这个目标。在标准软件包列表页面中，无法选择该 PTF 软件包。

1. 在 SUSE Manager Web UI 中，导航到**系统 › 系统列表**，然后选择要去除 PTF 的客户端。
2. 导航到**系统 › 软件 › PTF › 列出/去除**子选项卡。
3. 选择要去除的 PTF 软件包。
4. 单击 **[去除 PTF]**，然后在确认去除程序临时修复（PTF）页面上单击 **[确认]**。
5. 要查看结果，请导航到**系统 › 事件 › 历史记录**。

> 要去除 PTF，需要在客户端系统上安装 `libzypp` 和 `zypper` 的特殊版本。请运行 `zypper --help` 确认是否支持 `removeptf`。仅当满足此条件时，列出/去除选项卡才会显示。

如果应使用 API 去除 PTF，可以使用常规 `system.schedulePackageRemove` API 和代理软件包名称。

26.5. 在客户端上去除软件包的已修补版本

如果要使用控制台在客户端上直接去除 PTF，则需要使用特殊命令 `zypper removeptf`。所有其他方法要么会产生错误，要么可能导致非预期行为，例如从系统中去除重要软件包，致使系统不可用。

另请参见 https://www.suse.com/de-de/support/kb/doc/?id=000020596 了解命令行用法

Chapter 27. 查错

本章介绍了您在使用 SUSE Manager 时可能会遇到的一些常见问题及其解决方法。

27.1. 在公有云 (BYOS) 中设置使用不同数据磁盘的 SUSE Manager

问题：

在 SUSE Manager 设置期间重启动服务时，设置发生错误。

设置在重启动 Tomcat 时失败。

```
Write Settings
                                                                    Setup failed.
Setup script output
** Database: Shutting down spacewalk services that may be using DB.
** Database: Services stopped.  Clearing DB.
*** Progress: #
* Setting up users and groups.
* Performing initial configuration.
* Configuring apache SSL virtual host.
** /etc/apache2/vhosts.d/vhost-ssl.conf has been backed up to vhost-ssl.conf-swsave
* Configuring jabberd.
* Creating SSL certificates.
** SSL: Generating CA certificate.
** SSL: Generating server certificate.
** Database: Setting up report database.
** Database: --clear-db option used.  Clearing report database.
*** Progress: #
** Database: Installation complete.
* Report DB Configured.
* Update configuration in database.
* Setting up Cobbler..
* Deploying configuration files.
* Restarting services.
Tomcat failed to start properly or the installer ran out of tries.  Please check /var/log/tomcat/catalina.out or /var/log/tomcat/catalina.$(date +%Y-%m-%d).log for errors.
Error output
Warning: ALREADY_ENABLED: suse-manager-server
ERROR: spacewalk-setup failed
```

原因：

如果 SUSE Manager 设置为使用不同的磁盘来存储 cache、pgsql 和 spacewalk 数据，这些分区内的现有数据将会在新挂载点下被覆盖。

```
suma:~ # df -h | grep vg
/dev/mapper/vg--suma-spacewalk  1.5T  459G  1.1T  30% /var/spacewalk
/dev/mapper/vg--suma-pgsql      100G   17G   84G  17% /var/lib/pgsql
/dev/mapper/vg--suma-cache       50G  211M   50G   1% /var/cache
```

由于这个原因，某些服务（例如 tomcat）的数据因为符号链接损坏而丢失。

```
suma:~ # ll /etc/tomcat
total 236
lrwxrwxrwx 1 root root       26 Oct 16 08:36 Catalina -> /var/cache/tomcat/Catalina
-rw-r--r-- 1 root tomcat  13497 Oct 16 08:36 catalina.policy
-rw-r--r-- 1 root tomcat   7630 Oct 16 08:36 catalina.properties
drwxr-xr-x 2 root tomcat     83 Dec 13 18:48 conf.d
-rw-r--r-- 1 root tomcat   1400 Oct 16 08:36 context.xml
-rw-r--r-- 1 root tomcat   1149 Oct 16 08:36 jaspic-providers.xml
-rw-r--r-- 1 root tomcat   4450 Oct 16 08:36 logging.properties
-rw-r--r-- 1 root root     8124 Dec 13 18:48 server.xml
-rw-r--r-- 1 root root     7856 Dec 13 18:48 server.xml.2023-12-13T18:48:12.661
-rw-r----- 1 root tomcat   3224 Oct 16 08:36 tomcat-users.xml
-rw-r--r-- 1 root tomcat   1829 Oct 16 08:36 tomcat.conf
-rw-r--r-- 1 root tomcat 172577 Oct 16 08:36 web.xml
```

由于 SUSE Manager 云实例已设置了某些服务，当设置期间无法获取相应数据时，会导致服务无法正常重启

动。因此，设置会失败。

```
suma:~ # ll /var/cache
total 4
drwx------  3 root root   24 Jan 14 18:25 apparmor
drwxr-xr-x 36 man  man  4096 Jan 15 02:21 man
drwx------  2 root root    6 Jan 14 18:25 private
suma:~ #
```

应保留的实际数据：

```
suma:~ # umount /var/cache
suma:~ # ll /var/cache/
total 0
drwxr-x--- 2 wwwrun root     6 Oct 30 14:43 apache2
drwxr-xr-x 3 root   root    24 Jan 14 17:30 apparmor
drwxr-xr-x 2 root   root     6 Nov 24 12:20 cloudregister
drwxrwx--- 2 root   lp       6 Sep 12 12:19 cups
drwxr-xr-x 2 root   root   144 Dec 13 18:48 fontconfig
drwxr-xr-x 2 root   root   115 Dec 13 18:47 gio-2.0
drwx------ 2 root   root    23 Dec 13 18:48 ldconfig
drwxr-xr-x 2 man    man      6 Dec 13 18:48 man
drwx------ 2 root   root     6 Dec 13 18:47 private
drwxr-xr-x 3 wwwrun www     21 Dec 13 18:48 rhn
drwxr-x--- 4 root   salt    34 Dec 13 18:48 salt
drwxrwx--- 5 root   tomcat  46 Dec 13 18:47 tomcat
drwxr-xr-x 5 root   root    45 Jan 14 17:41 zypp
suma:~ # ll /var/cache/tomcat/
total 0
drwxrwxr-x 2 root tomcat 6 Oct 16 08:36 Catalina
drwxrwx--- 2 root tomcat 6 Oct 16 08:36 temp
drwxrwx--- 2 root tomcat 6 Oct 16 08:36 work
```

如何重新创建：

1. AWS 中置备的 SUSE Manager 服务器会针对 BYOS 使用相关的 AMI
2. 为 spacewalk、PostgreSQL 和 cache 使用单独的存储设备。 分区大小取决于要同步的储存库。
3. 使用 `yast2 susemanager_setup` 设置 SUSE Manager。

解决方法：

要解决该问题或避免该问题发生，请执行以下步骤将底层分区的数据复制到新分区中：

1. 创建备份分区

```
mkdir /bkp
```

2. 卸载受影响的分区，例如 /var/cache。

```
umount /var/cache
```

3. 检查该分区中的底层数据。以下命令应该会列出该目录中保留的实际数据。

```
ls -l /var/cache
```

4. 将数据复制到第 1 步中创建的备份分区中。

```
cp -prav /var/cache/* /bkp/
```

5. 使用选项 1 或 2 再次挂载分区：

```
（选项 1）  /dev/nvme0nxx /var/cache
（选项 2）  mount -a（如果 /etc/fstab 下有条目）
```

6. 将第 4 步中备份的数据复制到挂载的分区

```
cp -prav /bkp/* /var/cache/
```

7. 校验是否保留了数据

```
ls -l /var/cache/
```

8. 重复 SUSE Manager 设置过程

```
yast2 susemanager_setup
```

总结：

使用公有云中配置了不同数据分区的 SUSE Manager 时，请确保将这些目录中的现有数据复制到新分区。

27.2. 自动安装查错

根据您的基础通道，新的自动安装配置文件可能会订阅缺少必需软件包的通道。

要使自动安装可以正常进行，必须提供以下软件包：

- `pyOpenSSL`
- `rhnlib`

- `libxml2-python`
- `spacewalk-koan`

为了解决此问题，请先进行以下检查：

- 检查是否为您的组织和用户提供了与自动安装配置文件中的基础通道相关的工具软件通道。
- 检查是否为您的 SUSE Manager 提供了工具通道作为子通道。
- 检查关联的通道中是否提供了所需的软件包和所有依赖项：

27.3. 裸机系统查错

如果网络中的裸机系统不会自动添加到系统列表中，请先进行以下检查：

- 您必须已安装 `pxe-default-image` 软件包。
- 必须正确配置文件路径和参数。检查 `pxe-default-image` 提供的 `vmlinuz0` 和 `initrd0.img` 文件是否位于 `rhn.conf` 配置文件中指定的位置。
- 确保将裸机系统连接到 SUSE Manager 服务器的网络设备可正常运行，并且您可以从该服务器访问 SUSE Manager 服务器 IP 地址。
- 要置备的裸机系统必须在引导序列中启用 PXE 引导，并且必须未在尝试引导操作系统。
- 引导期间，DHCP 服务器必须响应 DHCP 请求。检查 PXE 引导消息，确保：
  - DHCP 服务器指派的是预期的 IP 地址
  - DHCP 服务器为要引导的 `next-server` 指派的是 SUSE Manager 服务器 IP 地址。
- 确保 Cobbler 正在运行，并且已启用发现功能。

如果您在系统引导后看到短暂显示的蓝色 Cobbler 菜单，则说明发现功能已启动。如果该过程未成功完成，请暂时禁用自动关闭功能以帮助诊断问题。要禁用自动关闭功能，请执行以下操作：

1. 使用方向键在 Cobbler 菜单中选择 `pxe-default-profile`，然后在计时器到期前按 Tab 键。
2. 使用集成编辑器添加内核引导参数 `spacewalk-finally=running`，然后按 Enter 继续引导。
3. 使用用户名 `root` 和口令 `linux` 进入外壳继续调试。

> 受技术所限，我们无法可靠地区分新裸机系统与先前已发现的系统。因此，建议您不要多次启动裸机系统，因为这会导致产生重复的配置文件。

27.4. 对生命周期已结束产品的引导储存库进行查错

同步受支持的产品时，会自动在 SUSE Manager Server 上创建及重新生成引导储存库。当产品到达生命周期结束日期且不再受支持时，如果您要继续使用此产品，就必须手动创建引导储存库。

有关引导储存库的详细信息，请参见 **Client-configuration › Bootstrap-repository**。

过程：创建生命周期已结束产品的引导储存库

1. 在 SUSE Manager Server 上的命令提示符下，以 root 身份使用 `--force`选项列出不受支持的可用引导储存库，例如：

```
mgr-create-bootstrap-repo --list --force
1. SLE-12-SP2-x86_64
2. SLE-12-SP3-x86_64
```

2. 创建引导储存库，并使用适当的储存库名称作为产品标签：

```
mgr-create-bootstrap-repo --create SLE-12-SP2-x86_64 --force
```

如果您不想手动创建引导储存库，可以检查您需要的产品和引导储存库是否有 LTSS。

27.5. 对克隆的 Salt 客户端进行查错

如果您曾经使用过超级管理程序克隆实用程序，并尝试注册克隆的 Salt 客户端，您可能会收到以下错误：

```
抱歉，找不到该系统。
```

发生该错误的原因是新的克隆系统与现有的已注册系统具有相同的计算机 ID。您可以手动调整此数据以修复该错误，然后便可成功注册克隆的系统。

有关详细信息和说明，请参见 **Administration › Troubleshooting**。

27.6. 对损坏的储存库进行查错

储存库元数据文件中的信息可能会损坏或过时。这可能会在更新客户端时造成问题。您可以通过去除再重新生成这些文件来解决此问题。生成新的储存库数据文件后，更新应该可以按预期进行。

过程：解决储存库数据损坏的问题

1. 去除 `/var/cache/rhn/repodata/<通道标签>` 中的所有文件。 如果您不知道通道标签是什么，可以在 SUSE Manager Web UI 中导航到**软件 › 通道 › 通道标签**找到它。
2. 从命令行重新生成文件：

```
spacecmd softwarechannel_regenerateyumcache <通道标签>
```

27.7. 对包含有冲突软件包的自定义通道进行查错

设置包含有冲突软件包的自定义通道时，某些功能（例如创建引导储存库）可能会导致未定义的行为，并使客户端注册失败。

例如，版本号较高的有冲突软件包可能会包含在引导储存库中。此类软件包（例如 `python3-zmq` 或 `zeromq`）可

能会导致创建引导储存库时出错，或者在客户端引导期间导致问题。

在父供应商通道下面添加自定义通道（例如 EPEL 通道）时，无法直接解决软件包冲突问题。此问题的解决方法是将自定义通道与供应商通道分开。需要在单独的树中创建自定义通道。如果需要将自定义通道作为子通道递送，可以使用内容生命周期管理 (CLM) 创建此类环境。可以从不同的树添加 CLM 项目中的源。如果使用这种方法，自定义通道将保留在构建的环境中的父项之下。但是，供应商通道树仍然不包含自定义通道和引导储存库。然后可以正常注册客户端。

将包含有冲突软件包的自定义通道（salt、zeromq 等）创建为子通道时，以下步骤可能有助于避免该问题：

过程：避免自定义通道中包含有冲突的软件包

1. 从父通道中去除作为子通道的自定义通道。有关详细信息，请参见 administration:custom-channels.pdf。
2. 在单独的树中创建自定义通道。有关详细信息，请参见 administration:custom-channels.pdf。 要在内容生命周期管理 (CLM) 中添加作为子通道的自定义通道，请执行以下操作：
   - 在 SUSE Manager Web UI 中，导航到**内容生命周期**，然后单击 **[创建项目]**。输入名称和标签。
   - 将源挂接到项目。使用所需的供应商通道和自定义通道。（分享使用 CentOS8 的示例）
   - 将环境添加到项目中。例如，使用 CentOS8。
   - 要构建环境，请单击 **[构建]** 按钮。这会创建一个包含供应商通道和自定义通道的环境，这些通道可与激活密钥相关联并用于引导客户端。
3. 重要说明：在 CLM 项目中，建议添加一个过滤器用于排除有问题或有冲突的软件包。否则会在客户端更新期间安装版本号较高的有冲突软件包。有关过滤的详细信息，请参见 administration:content-lifecycle-examples.pdf。
4. 要将最新补丁添加到 CLM 环境（包含供应商通道和自定义通道），请在项目中单击 **[构建]** 按钮。需要执行此操作才能重构建环境。
   - 有关 CLM 的详细信息，请参见 **Administration › Content-lifecycle**。

> 如果直接在 Red Hat Enterprise Linux 客户端（或 SUSE Liberty Linux、CentOS、Oracle Linux 等兼容系统）上使用 Extra Packages for Enterprise Linux (EPEL)，将会安装 EPEL 提供的 Salt 软件包，这会丢失 SUSE Manager 提供的 Salt 软件包中包含的某些功能。此问题非常严重，因为这样将会生成一个包含非 SUSE Salt 软件包的引导储存库。因此，系统不支持这样的使用场景。如果您需要启用 EPEL 储存库，请务必提前过滤掉 EPEL 提供的 Salt 软件包（例如，在**软件 › 管理 › 通道 › EPEL › 软件包**中去除 Salt 软件包）。

27.8. 对禁用 FQDNS grain 时出现的问题进行查错

FQDNS grain 会返回系统中所有完全限定 DNS 服务的列表。通常很快就能完成这些信息的收集，但如果 DNS 设置配置错误，花费的时间可能会长很多。在某些情况下，客户端会变成无响应状态或者会崩溃。

为了防止发生此问题，您可以使用 Salt 标志来禁用 FQDNS grain。如果禁用 grain，您便可以使用网络模块提供 FQDNS 服务，而不会面临客户端变成无响应状态的风险。

> 这仅适用于较旧的 Salt 客户端。如果您是最近注册 Salt 客户端的，FQDNS grain 默认会禁用。

在 SUSE Manager Server 上的命令提示符下，使用以下命令禁用 FQDNS grain：

```
salt '*' state.sls util.mgr_disable_fqdns_grain
```

此命令会重启动每个客户端并生成服务器需要处理的 Salt 事件。如果您的客户端非常多，可以改用批处理模式执行该命令：

```
salt --batch-size 50 '*' state.sls util.mgr_disable_fqdns_grain
```

等待批处理命令执行完。请不要按 `Ctrl`+`C` 中断该过程。

27.9. 磁盘空间查错

磁盘空间不足可能会对 SUSE Manager 数据库和文件结构造成严重影响，在大多数情况下，这种影响不可恢复。SUSE Manager 会监视特定目录的可用空间，在有问题时会发出警报（可配置）。有关空间管理的详细信息，请参见 **Administration › Space-management**。

可以通过去除未使用的软件通道来恢复磁盘空间。有关如何删除供应商通道的说明，请参见**Administration › Channel-management**。有关如何删除自定义通道的说明，请参见 **Administration › Custom-channels**。

您还可以检查自定义通道的同步频率。有关如何处理自定义通道同步的说明，请参见 administration:custom-channels.pdf。

还可以通过清理未使用的激活密钥、内容生命周期项目和客户端注册来恢复磁盘空间。还可以去除多余的数据库项：

过程：去除多余的数据库项

1. 使用 `spacewalk-data-fsck` 命令列出所有多余的数据库项。
2. 使用 `spacewalk-data-fsck --remove` 命令删除这些项。

27.10. 防火墙查错

如果您使用的防火墙阻止了传出流量，它可能会拒绝或丢弃网络请求。如果该防火墙设置为丢弃，则与 SUSE Customer Center 同步可能会超时。

之所以发生这种情况，是因为同步进程需要访问为非 SUSE 客户端（而不仅仅是 SUSE Customer Center）提供软件包的第三方储存库。当 SUSE Manager Server 尝试访问这些储存库以检查它们是否有效时，防火墙会丢弃请求，并且同步进程会继续等待响应，直到超时。

如果发生这种情况，同步将持续很长时间，然后失败，并且您的非 SUSE 产品不会显示在产品列表中。

可以通过多种不同的方法解决此问题。

最简单的方法是将防火墙配置为允许访问非 SUSE 储存库所需的 URL。这样，同步进程就能访问这些 URL 并成功完成。

如果不能允许外部流量，请将防火墙配置为拒绝来自 SUSE Manager 的请求，而不是丢弃。这会拒绝对第三方 URL 的请求，因此同步会提前失败而不是超时，并且产品不会显示在列表中。

如果您无权配置防火墙，可以考虑在 SUSE Manager Server 上单独设置一个防火墙。

27.11. 对通过 WAN 连接在 SUSE Manager Server 与 Proxy 之间同步时间过长的问题进行查错

根据在 WebUI 中或通过 API 调用对发行套件或系统设置执行的更改，可能需要使用 `cobbler sync` 命令将 SUSE Manager 服务器中的文件传输到 SUSE Manager Proxy 系统。为此，Cobbler 将使用 `/etc/cobbler/settings` 中指定的代理列表。

`cobbler sync` 在设计上无法仅同步已更改的或最近添加的文件。

实际情况是，执行 `cobbler sync` 会触发将 `/srv/tftpboot` 目录完全同步到 `/etc/cobbler/settings` 中配置的所有已指定代理的操作。此命令还会受到相关系统之间 WAN 连接延迟的影响。

根据 `/var/log/cobbler/` 中的日志，同步过程可能需要很长时间才能完成。

例如，该过程开始时间为：

```
Thu Jun  3 14:47:35 2021 - DEBUG | running python triggers from
/var/lib/cobbler/triggers/task/sync/pre/*
Thu Jun  3 14:47:35 2021 - DEBUG | running shell triggers from
/var/lib/cobbler/triggers/task/sync/pre/*
```

结束时间为：

```
Thu Jun  3 15:18:49 2021 - DEBUG | running shell triggers from
/var/lib/cobbler/triggers/task/sync/post/*
Thu Jun  3 15:18:49 2021 - DEBUG | shell triggers finished successfully
```

传输量大约为 1.8 GB。传输花费了将近 30 分钟。

相比之下，复制一个与 `/srv/tftboot` 大小相同的大文件只需几分钟即可完成。

改用基于 `rsync` 的方法在 SUSE Manager Server 与 Proxy 之间复制文件可能有助于减少传输量和等待时间。

可以从 https://suse.my.salesforce.com/sfc/p/1i000000gLOd/a/1i000000ll5B/B2AmvIJN2_JsAyjTQzCVP_x5ioVgd0bYN9X9NpMugS8 下载用于完成此任务的脚本。

该脚本不接受命令行选项。在运行该脚本之前，您需要手动编辑它并正确设置 `SUMAHOSTNAME`、`SUMAIP` 和 `SUMAPROXY1` 变量，使其能够正常运行。

> 不支持调整该脚本的个别设置。该脚本及其包含的注释旨在提供传输过程以及要考虑的步骤的概述。如需进一步的帮助，请联系 SUSE 咨询部门。

对于以下情况，最好使用建议的脚本用法：

- SUSE Manager 代理系统是通过 WAN 连接的；
- `/srv/tftboot` 包含大量发行套件文件和客户端 PXE 引导文件，总共有数千个文件；
- 已禁用 `/etc/cobbler/settingsl` 中的任一代理，否则 SUSE Manager 会继续将内容同步到代理。

```
#proxies:
# - "sumaproxy.sumaproxy.test"
# - "sumaproxy2.sumaproxy.test"
```

过程：分析新的同步速度

1. 为 SUSE Manager 与相关系统之间的 TCP 流量创建转储。
   - 在 SUSE Manager Server 上：

     ```
     tcpdump -i ethX -s 200 host <SUSE Manager Proxy 的 IP 地址> and not ssh
     ```

   - 在 SUSE Manager Proxy 上：

     ```
     tcpdump -i ethX -s 200 host <SUSE Manager 的 IP 地址> and not ssh
     ```

   - 这样就只会捕获大小为 200 的软件包，但足以运行分析。
   - 将 ethX 调整为由 SUSE Manager 用来与代理通讯的相应网络接口。
   - 最后，不会捕获 ssh 通讯，从而进一步减少了软件包的数量。
2. 开始 Cobbler 同步。
   - 要强制同步，请先删除 Cobbler json 缓存文件，然后发出 Cobbler 同步命令：

     ```
     rm /var/lib/cobbler/pxe_cache.json
     cobbler sync
     ```

3. Cobbler 完成后，停止 TCPdumps。
4. 使用 Wireshark 打开 TCPdumps，转到 `Statistics（统计信息）> Conversations（对话）`，并等待分析转储。
5. 切换到“TCP”选项卡。此选项卡上显示的数字是在 SUSE Manager 与 SUSE Manager Proxy 之间捕获的对话总数。
6. 找到列 `Duration（持续时间）`。
   - 首先按升序排序，找出传输文件所花费的最短时间。
   - 继续按降序排序，找出大文件传输时间的最大值，例如内核和 initrd 传输。

忽略端口 4505 和 4506，因为它们用于 Salt 通讯。

TCPdumps 分析结果表明，将大小约为 1800 字节的小文件从 SUSE Manager Server 传输到 Proxy 大约花费了 0.3 秒。

此处的大文件不多，而大量的小文件导致建立了大量连接，因为每传输一个文件就要创建新的 TCP 连接。

因此，在知道最短传输时间和所需连接数（在本示例中大约为 5000）的情况下，可以大致估算出总传输时间：5000 * 0.3 / 60 = 25 分钟。

27.12. 非活动客户端查错

某个 Taskomatic 作业会定期 ping 客户端以确保它们保持连接状态。有 24 小时或更长时间未响应 Taskomatic 签入的客户端被视为非活动客户端。要在 Web UI 中查看非活动客户端的列表，请导航到**系统 › 系统列表 › 非活动**。

客户端可能由于多种原因而进入非活动状态：

- 客户端无权使用任何 SUSE Manager 服务。
- 在传统客户端上，`rhnsd` 服务已禁用。
- 客户端位于不允许 HTTPS 连接的防火墙后面。
- 客户端位于配置不当的代理后面。
- 客户端正在与其他 SUSE Manager Server 通讯，或者连接配置不当。
- 客户端不在可以与 SUSE Manager Server 通讯的网络中。
- 防火墙阻止了客户端与 SUSE Manager Server 之间的通讯。
- Taskomatic 配置不当。

有关客户端与服务器的连接的详细信息，请参见 **Client-configuration › Contact-methods-intro**。

有关配置端口的详细信息，请参见 **Installation-and-upgrade › Ports**。

有关防火墙查错的详细信息，请参见 **Administration › Troubleshooting**。

27.13. 服务器间同步查错

服务器间同步使用缓存来管理 ISS 主服务器和从属服务器。这些缓存容易出现 bug，导致创建无效的项。在这种情况下，即使更新到解决了 bug 的版本，这些 bug 也还可能出现，因为缓存仍在使用无效的项。如果您升级到新版 ISS 后仍然遇到问题，请清除所有缓存，以确保不再有旧项造成问题。

缓存错误可能导致同步失败并出现各种错误，但错误消息通常会报告如下内容：

考虑去除 /var/cache/rhn/satsync/* 中的 satellite-sync 缓存并使用相同的选项重新运行 satellite-sync。

可以通过删除 ISS 主服务器和 ISS 从属服务器上的缓存来解决此问题，这样，同步即可成功完成。

过程：解决 ISS 缓存错误

1. 在 ISS 主服务器上的命令提示符下，以 root 身份删除主服务器的缓存文件：

```
rm -rf /var/cache/rhn/xml-*
```

2. 重启动服务：

```
rcapache2 restart
```

3. 在 ISS 主服务器上的命令提示符下，以 root 身份删除从属服务器的缓存文件：

```
rm -rf /var/cache/rhn/satsync/*
```

4. 重启动服务：

```
rcapache2 restart
```

27.14. 本地颁发者证书查错

某些较旧的引导脚本会在错误的位置创建本地证书的链接。这会导致 zypper 返回有关本地颁发者证书的无法识别的错误。您可以通过检查 `/etc/ssl/certs/` 目录来确保正确创建本地颁发者证书的链接。如果您遇到此问题，应考虑更新引导脚本以确保 zypper 按预期运行。

27.15. 登录超时查错

默认情况下，SUSE Manager Web UI 要求用户在 30 分钟后重新登录。根据您的环境，可能需要调整登录超时值。

要调整该值，需要同时在 `rhn.conf` 和 `web.xml` 中进行更改。确保在 `/etc/rhn/rhn.conf` 中设置以秒为单位的值，在 `web.xml` 中设置以分钟为单位的值。这两个值必须表示相同的时间。

例如，要将超时值更改为一小时，请将 `rhn.conf` 中的值设置为 3600 秒，将 `web.xml` 中的值设置为 60 分钟。

过程：调整 Web UI 登录超时值

1. 停止服务：

```
spacewalk-service stop
```

2. 打开 `/etc/rhn/rhn.conf` 并添加或编辑下面一行内容，以包含以秒为单位的新超时值：

```
web.session_database_lifetime = <以秒为单位的超时值>
```

3. 保存并关闭该文件。
4. 打开 `/srv/tomcat/webapps/rhn/WEB-INF/web.xml` 并添加或编辑下面一行内容，以包含以分钟为单位的新超时值：

```
<session-timeout>Timeout_Value_in_Minutes</session-timeout>
```

5. 保存并关闭该文件。
6. 重启动服务：

```
spacewalk-service start
```

27.16. 邮件配置查错

为确保邮件通讯安全，您可以在 `/etc/rhn/rhn.conf` 中启用身份验证，定义用户名和口令，并启用 `SSL` 或 `STARTLS`：

```
java.smtp_port = 整数（默认值：25）
java.smtp_auth = true/false（默认值：false）
java.smtp_ssl = true/false（默认值：false）
java.smtp_starttls = true/false（默认值：false）
java.smtp_user = 字符串（默认值：null）
java.smtp_pass = 字符串（默认值：null）
```

要为 SMTP 服务器通信的连接超时设置更高的值，可以在 `/etc/rhn/rhn.conf` 中设置以下参数：

```
java.smtp_timeout = integer (default: 5000)
java.smtp_connection_timeout = integer (default: 5000)
java.smtp_write_timeout = integer (default: 5000)
```

27.17. 对使用 noexec 挂载 /tmp 时出现的问题进行查错

Salt 从客户端文件系统的 `/tmp` 中运行远程命令。因此，切勿使用 `noexec` 选项挂载 `/tmp`。另一个解决此问题的方法是，使用为 Salt 服务指定的 `TMPDIR` 环境变量覆盖临时目录路径，使其指向未设置 `noexec` 选项的目录。建议使用 systemd 插入配置文件 `/etc/systemd/system/venv-salt-minion.service.d/10-TMPDIR.conf`（如果使用了 Salt 捆绑包）或 `/etc/systemd/system/salt-minion.service.d/10-TMPDIR.conf`（如果客户端上使用了 `salt-minion`）。插入配置文件内容的示例如下：

```
[Service]
Environment=TMPDIR=/var/tmp
```

27.18. 对使用 noexec 挂载 /var/tmp 时出现的问题进行查错

Salt SSH 使用 `/var/tmp` 在安装了绑定 Python 的客户端上部署 Salt 捆绑包和执行 Salt 命令。因此，切勿使用 `noexec` 选项挂载 `/var/tmp`。无法通过 Web UI 引导使用 `noexec` 选项挂载 `/var/tmp` 的客户端，因为引导过程是使用 Salt SSH 来访问客户端的。

27.19. 对“磁盘空间不足”错误进行查错

在开始迁移之前，请检查可用磁盘空间。我们建议将 /var/spacewalk 和 /var/lib/pgsql 存放于不同的 XFS 文件系统中。

设置单独的文件系统时，编辑 /etc/fstab 并去除 /var/lib/pqsql 子卷。重引导服务器以应用更改。

要获取有关升级问题的详细信息，请查看迁移日志文件。该日志文件是您要升级的系统上的 /var/log/rhn/migration.log。

27.20. 通知查错

通知消息的默认有效期为 30 天，此期限过后会从数据库中删除消息，无论其阅读状态如何。要更改此值，请在 /etc/rhn/rhn.conf 中添加或编辑下面一行内容：

```
java.notifications_lifetime = 30
```

要启用或禁用某个通知类型，请在 /etc/rhn/rhn.conf 中添加或编辑下面一行内容：

```
java.notifications_type_disabled = OnboardingFailed,ChannelSyncFailed,\
  ChannelSyncFinished,CreateBootstrapRepoFailed,StateApplyFailed,\
  PaygAuthenticationUpdateFailed,EndOfLifePeriod,SubscriptionWarning
```

有关默认设置和配置选项，请参见 usr/share/rhn/config-defaults/rhn_java.conf 模板文件。

27.21. 对启用 OES 储存库时出现的问题进行查错

要在 SUSE Manager Server 上启用 Open Enterprise Server (OES)，请按照所述的过程进行操作。

过程：启用 OES 储存库

1. 确保您拥有 Microfocus 提供的有权访问 OES 的镜像身份凭证。
2. 登录到 SUSE Manager Server。
3. 转到管理 > 安装向导 > 组织身份凭证。
4. 确保您已拥有 SUSE Manager 的 SUSE 身份凭证。
5. 选择用于添加新身份凭证的选项，然后键入 Microfocus 身份凭证。
6. 转到管理 > 安装向导 > 组织身份凭证，然后等待刷新操作完成。
7. OES 应会显示在已刷新的产品列表中。您现在可以像启用任何其他产品一样启用它。

有关 OES 的详细信息，请参见 https://www.microfocus.com/documentation/open-enterprise-server/。

27.22. OSAD 和 jabberd 查错

在某些情况下，jabber 可以打开的最大文件数量少于连接的 OSAD 客户端数量。

如果出现这种情况，OSAD 客户端将无法联系 SUSE Manager Server，并且 jabberd 会花费过多的时间在端口 5222 上做出响应。

> 仅当您使用 OSAD 连接的客户端数超过 8192 个时，才需要采取此修复措施。对于这种情况，我们建议您考虑改用 Salt 客户端。有关微调大规模安装的详细信息，请参见 **Specialized-guides › Salt**。

可以通过编辑 jabberd 本地配置文件来增加 jabber 可用的文件数。该文件的默认路径为 `/etc/systemd/system/jabberd.service.d/override.conf`。

过程：调整最大文件计数

1. 在命令提示符下，以 root 身份打开本地配置文件进行编辑：

```
systemctl edit jabberd
```

2. 添加或编辑以下部分：

```
[Service]
LimitNOFILE=<软限制>:<硬限制>
```

要选择的值因环境而异。例如，如果您有 9500 个客户端，可将软限制值增大 100，即 9600，并将硬限制值增大 1000，即 10500：

```
[Unit]
LimitNOFILE=
LimitNOFILE=9600:10500
```

3. 保存该文件并退出编辑器。

> systemctl 文件的默认编辑器是 vim。要保存文件并退出，请按 `Esc` 进入常规模式，键入 `:wq` 并按 `Enter`。

确保同时更新 `/etc/jabberd/c2s.xml` 中的 `max_fds` 参数。例如：`<max_fds>10500</max_fds>`

文件数软限制是单个进程可以打开的文件数上限。在 SUSE Manager 中，资源消耗量最高的进程是 `c2s`，它为每个客户端打开一个连接。此处额外添加了 100 个文件，以弥补所需的任何非连接文件，使 `c2s` 能够正常运行。硬限制适用于属于 jabber 的所有进程，此外还考虑了从路由器、`c2s` 和 `sm` 进程打开的文件。

27.23. 对软件包不一致问题进行查错

当客户端上的软件包被锁定时，SUSE Manager Server 可能无法正确确定适用的补丁集。如果发生这种情况，软件包更新会显示在 Web UI 中，但不会显示在客户端上，并且尝试更新客户端会失败。检查软件包锁定和排

除列表，以确定是否在客户端上锁定或排除了软件包。

在客户端上，检查软件包锁定和排除列表，以确定是否已锁定或排除软件包：

- 在扩展支持平台上，检查 `/etc/yum.conf` 并搜索 `exclude=`。
- 在 SUSE Linux Enterprise 和 openSUSE 上，使用 `zypper locks` 命令。

27.24. 对通过代理获取储存库信息时出现的问题进行查错

在某些情况下，代理上的 `squid` 缓存会损坏。如果发生这种情况，在连接到代理的客户端上获取软件包或储存库元数据会失败，并出现各种可能的错误消息。

在常规代理或容器代理上，清理 `squid` 缓存的方式不同。

对于常规代理，请在代理计算机上执行以下过程：

```
systemctl stop squid
rm -rf /var/cache/squid/*
squid -z
systemctl start squid
```

对于使用 `podman` 运行的容器代理，请在主机计算机上执行以下过程：

```
systemctl stop uyuni-proxy-pod
podman volume rm uyuni-proxy-squid-cache
systemctl start uyuni-proxy-pod
```

27.25. 对将 Grain 传递给启动事件时出现的问题进行查错

Salt 客户端每次启动时都会将 `machine_id` grain 传递给 SUSE Manager。SUSE Manager 使用此 grain 确定客户端是否已注册。此过程需要进行同步 Salt 调用。同步 Salt 调用会阻止其他进程，因此如果您有大量客户端同时启动，该过程可能会造成很严重的延迟。

为了解决此问题，Salt 中引入了一项新功能来避免进行单独的同步 Salt 调用。

要使用此功能，您可以在支持该功能的客户端上向客户端配置中添加一个配置参数。

如果想要更轻松地完成此过程，您可以使用 `mgr_start_event_grains.sls` 助手 Salt 状态。

> 这仅适用于已注册的客户端。如果您是最近注册 Salt 客户端的，系统默认会添加此配置参数。

在 SUSE Manager Server 上的命令提示符下，使用以下命令启用 `start_event_grains` 配置助手：

```
salt '*' state.sls util.mgr_start_event_grains
```

此命令会在客户端的配置文件中添加所需的配置，并在客户端重启动时应用更改。如果您的客户端非常多，可

以改用批处理模式执行该命令：

```
salt --batch-size 50 '*' state.sls mgr_start_event_grains
```

27.26. PAYG 查错

检查身份凭证

- 如果脚本无法收集身份凭证，将会在日志和 Web UI 中提供正确的错误消息。
- 如果身份凭证无法工作，`reposync` 应该会显示正确的错误消息。

使用 `registercloudguest`

- 刷新或更改 `registercloudguest` 与公有云更新基础架构的连接不应影响身份凭证的使用。
- 如果未使用 cloud guest 命令注册新的云连接，运行 `registercloudguest --clean` 将会导致发生问题。

27.27. 配置代理后端的 Pay-as-you-go

为了识别虚拟机是否为 PAYG 类型，SUSE Manager 需要使用 `sudo` 来运行 `instance-flavor-check` 工具。

如果客户使用的是 http 代理，他们需要确保通过 `sudo` 正确管理此设置，因为默认情况下会忽略大多数环境变量。

要实现此目的，一种方法是添加包含以下内容的 `/etc/sudoers.d/keep_proxy.conf` 文件：

```
# Preserve any possible proxy configuration
Defaults env_keep += "http_proxy https_proxy no_proxy"
```

这可确保与代理相关的环境变量能够在权限升级期间保留。

27.28. 代理连接和 FQDN 查错

有时，通过代理连接的客户端会显示在 Web UI 中，但不会显示它们是通过代理连接的。如果您连接时使用的不是完全限定的域名 (FQDN)，而代理对 SUSE Manager 而言是未知的，就可能发生此情况。

要更正此行为，请在代理上的客户端配置文件中指定其他 FQDN 作为 grain：

```
grains:
  susemanager:
    custom_fqdns:
      - name.one
      - name.two
```

27.29. 对注册克隆的客户端时出现的问题进行查错

如果您使用 SUSE Manager 来管理虚拟机，您可能发现创建 VM 的克隆版本会很有用。克隆版本是使用主磁盘（与现有磁盘完全相同的副本）的 VM。

虽然克隆 VM 可以节省大量时间，但磁盘上复制的标识信息有时会导致问题。

如果您有一个已注册的客户端，并创建了该客户端的克隆版本，在尝试注册该克隆版本时，您可能希望 SUSE Manager 将原始客户端和克隆版本注册为两个不同的客户端。但是，如果原始客户端和克隆版本中的计算机 ID 相同，则 SUSE Manager 会将这两个客户端注册为一个系统，并且现有客户端数据将由克隆版本的数据重写。

可以通过更改克隆版本的计算机 ID 来解决此问题，以便 SUSE Manager 将它们识别为两个不同的客户端。

此过程的每个步骤都在克隆的客户端上执行。此过程不会对原始客户端进行操作，原始客户端仍保持注册到 SUSE Manager。

过程：解决克隆的 Salt 客户端中的重复计算机 ID

1. 在克隆的计算机上，更改主机名和 IP 地址。 确保 `/etc/hosts` 包含您所做的更改和正确的主机项。
2. 对于支持 systemd 的发行套件：如果您的计算机具有相同的计算机 ID，请以 root 身份删除复制的每个客户端上的文件，然后重新创建这些文件：

```
rm /etc/machine-id
rm /var/lib/dbus/machine-id
rm /var/lib/zypp/AnonymousUniqueId
dbus-uuidgen --ensure
systemd-machine-id-setup
```

3. 对于不支持 systemd 的发行套件：以 root 身份从 dbus 生成计算机 ID：

```
rm /var/lib/dbus/machine-id
rm /var/lib/zypp/AnonymousUniqueId
dbus-uuidgen --ensure
```

4. 如果您的客户端仍然具有相同的 Salt 客户端 ID，请删除每个客户端上的 `minion_id` 文件（这样就会使用在客户端重启动时重新生成的 FQDN）。对于 Salt 受控端客户端：

```
rm /etc/salt/minion_id
rm -rf /etc/salt/pki
```

对于 Salt 捆绑包客户端：

```
rm /etc/venv-salt-minion/minion_id
rm -rf /etc/venv-salt-minion/pki
```

5. 从初始配置页面中删除接受的密钥并从 SUSE Manager 中删除系统配置文件，然后使用以下命令重启动客户端：

```
service salt-minion restart
```

6. 重新注册客户端。 每个客户端现在都有一个不同的 `/etc/machine-id`，并且应会正确显示在系统概览页面上。

过程：解决克隆的传统客户端中的重复计算机 ID

1. 在克隆的计算机上，更改主机名和 IP 地址。 确保 `/etc/hosts` 包含您所做的更改和正确的主机项。
2. 在 Red Hat Enterprise Linux Server 6 和 SUSE Linux Enterprise 11 上使用以下命令停止 `rhnsd` 守护程序：

   ```
   /etc/init.d/rhnsd stop
   ```

   或者，在基于 systemd 的较新系统上使用以下命令：

   ```
   service rhnsd stop
   ```

3. 使用以下命令停止 `osad`：

   ```
   /etc/init.d/osad stop
   ```

   或：

   ```
   service osad stop
   ```

   或：

   ```
   rcosad stop
   ```

4. 去除 `osad` 身份验证配置文件和系统 ID：

   ```
   rm -f /etc/sysconfig/rhn/{osad-auth.conf,systemid}
   ```

5. 删除包含计算机 ID 的文件：
   - SLES 12：

     ```
     rm /etc/machine-id
     rm /var/lib/dbus/machine-id
     dbus-uuidgen --ensure
     systemd-machine-id-setup
     ```

   - SLES 11：

     ```
     suse_register -E
     ```

6. 去除身份凭证文件：
   - SLES 客户端：

     ```
     rm -f /etc/zypp/credentials.d/{SCCcredentials,NCCcredentials}
     ```

- Red Hat Enterprise Linux 客户端：

```
rm -f /etc/NCCcredentials
```

7. 重新运行引导脚本。 现在应会在 SUSE Manager 中看到克隆的系统，而不会覆盖该系统的源系统。

27.30. 对在 Web UI 中注册失败且未显示任何错误的问题进行查错

在 Web UI 中进行初始注册时，所有 Salt 客户端使用的都是 Salt SSH。

由其性质决定，Salt SSH 客户端不会向服务器回报错误。

不过，Salt SSH 客户端会将日志存储在本地的 `/var/log/salt-ssh.log` 中，您可以在其中检查错误。

27.31. 对在删除传统客户端后将其注册为 Salt 受控端时出现的问题进行查错

这不是有效的方案。通常您应将传统客户端迁移为 Salt 受控端，而不是删除该客户端。Salt 会自动检测到您有一个传统客户端并会自行执行必要的更改。但如果您已删除传统客户端，现在想要重新将其注册为 Salt 受控端，则必须在将其注册为 Salt 受控端之前在客户端上执行以下步骤：

1. 去除下面的文件：

```
/etc/sysconfig/rhn/systemid
```

2. 去除下面的软件包：

```
zypp-plugin-spacewalk
```

27.32. 对注册传统 Red Hat 客户端时出现的问题进行查错

传统的 Red Hat Enterprise Linux 7 和 SLES Expanded Support 7 客户端需要一些未签名的软件包才能正常与 SUSE Manager 配合运行，因此这些客户端类型的自定义通道通常会取消设置 `gpgcheck` 标志。但是，`rhnplugin.conf` 文件会覆盖此设置并启用 GPG 检查。

这意味着，在注册传统的 Red Hat Enterprise Linux 7 和 SLES Expanded Support 7 客户端时，客户端不会从自定义通道安装未签名的软件包，即使在自定义通道中禁用了 `gpgcheck`。

要解决此问题，请编辑 `/etc/yum/pluginconf.d/rhnplugin.conf` 文件并禁用 GPG 检查，以启用未签名软件包的安装并使客户端能够按预期运行。

27.33. 对 Red Hat CDN 通道和多个证书进行查错

有时，Red Hat 内容分发网络(CDN) 通道会提供多个证书，而 SUSE Manager Web UI 只能导入单个证书。如果 CDN 提供的证书与 SUSE Manager Web UI 已知的证书不同，即使该证书准确无误，验证也会失败，并且访问

储存库的权限会被拒绝。收到的错误消息如下：

```
[错误]
储存库 '<repo_name>' 无效。
<repo.pem> 在指定的 URL 未找到有效元数据
历史记录：
 - [|] 尝试从 '<repo.pem>' 读取数据时出错
 - 访问 '<repo.pem>' 的权限被拒绝。
请检查为此储存库定义的 URL 是否指向有效储存库。
由于发生上述错误，正在跳过储存库 '<repo_name>'。
由于发生错误，无法刷新储存库。
HH:MM:SS RepoMDError：无法访问储存库。可能未导入储存库 GPG 密钥
```

要解决此问题，请将所有有效的证书合并到单个 `.pem` 文件中，然后重构建证书以供 SUSE Manager 使用：

过程：解析多个 Red Hat CDN 证书

1. 在 Red Hat 客户端上的命令提示符下，以 root 身份将 `/etc/pki/entitlement/` 中的所有当前证书合并到单个 `rh-cert.pem` 文件中：

   ```
   cat 866705146090697087.pem 3539668047766796506.pem redhat-entitlement-
   authority.pem > rh-cert.pem
   ```

2. 将 `/etc/pki/entitlement/` 中的所有当前密钥合并到单个 `rh-key. pem` 文件中：

   ```
   cat 866705146090697087-key.pem 3539668047766796506-key.pem > rh-key.pem
   ```

现在，您可以按照**Client-configuration › Clients-rh-cdn**中的说明将新证书导入 SUSE Manager Server。

27.34. SUSE Manager Server 重命名查错

如果您在本地更改了 SUSE Manager Server 的主机名，SUSE Manager 安装将无法正常进行。这是因为尚未在数据库中做出相应更改，因而这些更改无法从您的客户端和任何代理传播出来。

如果您需要更改 SUSE Manager 服务器的主机名，可以使用 `spacewalk-hostname-rename` 脚本来更改。此脚本会更新 PostgreSQL 数据库以及 SUSE Manager 的内部结构中的设置。

`spacewalk-hostname-rename` 脚本是 `spacewalk-utils` 软件包的一部分。

该脚本的唯一必需参数是为 SUSE Manager Server 新配置的 IP 地址。

过程：重命名 SUSE Manager Server

1. 在 DNS 服务器上，本地和远程更改系统级别的服务器的网络设置。 您还需要提供用于反向名称解析的配置设置。更改网络设置的方式与重命名任何其他系统的方式相同。
2. 重引导 SUSE Manager Server 以使用新网络配置并确保主机名更改。
3. 结合服务器的公共 IP 地址运行脚本 `spacewalk-hostname-rename`。 如果服务器未使用新主机名，则该脚本会失败。请注意，此脚本会刷新所有 Salt 客户端的 pillar 数据：运行时间取决于注册的客户端数量。

4. **如果通过 SUSE Manager 代理管理客户端，请跳过此步骤。** 重新配置直接管理的客户端，确保它们知道新主机名和 IP 地址。 在 Salt 客户端配置文件中，必须指定新 Salt 主控端（SUSE Manager 服务器）的名称（文件名为 `/etc/venv-salt-bundle/minion`，如果您未使用 Salt 捆绑包，则为 `/etc/salt/minion`）：

```
master: <新主机名>
```

5. 重启动 `venv-salt-minion` 服务（如果使用 Salt 捆绑包）：

```
systemctl restart venv-salt-minion
```

或 `salt-minion` 服务（如果未使用 Salt 捆绑包）：

```
systemctl restart salt-minion
```

6. 要将主机名完全传播到 Salt 客户端配置，请应用 Highstate。应用 Highstate 会更新储存库 URL 中的主机名。

> 必须重新配置所有代理。必须将新服务器证书和密钥复制到代理上，并且必须运行 `configure-proxy.sh` 脚本。有关配置代理的详细信息，请参见 **Installation-and-upgrade › Proxy-setup**。

直接连接的传统客户端使用 `/etc/sysconfig/rhn/up2date` 配置文件，必须更改此文件。使用重新激活密钥可以重新注册传统客户端（如果有）。有关详细信息，请参见 **Client-configuration › Registration-cli**。

> 如果通过某个代理使用 PXE 引导，则必须检查该代理的配置设置。在该代理上，运行 `configure-tftpsync.sh` 设置脚本并输入请求的信息。有关详细信息，请参见 **Installation-and-upgrade › Proxy-setup**。

27.35. 对重新尝试设置目标系统时出现的问题进行查错

如果需要重新尝试设置目标系统，请执行以下步骤：

1. 删除 `/root/.MANAGER_SETUP_COMPLETE`。
2. 停止 PostgreSQL 并去除 `/var/lib/pgsql/data`。
3. 将目标系统主机名设置为与源系统主机名匹配的名称。
4. 检查 `/etc/hosts` 文件，并根据需要更正。
5. 检查目标系统中的 `/etc/setup_env.sh`，并确保已设置数据库名称：

```
MANAGER_DB_NAME='susemanager'
```

6. 重引导目标系统。
7. 再次运行 `mgr-setup`。

27.36. RPC 超时查错

由于网络速度缓慢或网络链接断开，RPC 连接有时会超时。这会导致软件包下载或批处理作业挂起或运行时间超过预期。您可以通过编辑配置文件来调整 RPC 连接可以花费的最长时间。虽然这不能解决网络问题，但可以使进程失败而不是挂起。

过程：解决 RPC 连接超时

1. 在 SUSE Manager Server 上，打开 `/etc/rhn/rhn.conf` 文件并设置最大超时值（以秒为单位）：

```
server.timeout =`数字`
```

2. 在 SUSE Manager Proxy 上，打开 `/etc/rhn/rhn.conf` 文件并设置最大超时值（以秒为单位）：

```
proxy.timeout =`数字`
```

3. 在使用 zypper 的 SUSE Linux Enterprise Server 客户端上，打开 `/etc/zypp/zypp.conf` 文件并设置最大超时值（以秒为单位）：

```
## 有效值：[0,3600]
## 默认值：180
download.transfer_timeout = 180
```

4. 在使用 yum 的 Red Hat Enterprise Linux 客户端上，打开 `/etc/yum.conf` 文件并设置最大超时值（以秒为单位）：

```
timeout =`数字`
```

如果您将 RPC 超时限制为小于 `180` 秒，可能会中止完全正常的操作。

27.37. 对 Salt 客户端显示为关闭状态的问题和 DNS 设置进行查错

即使 Salt 客户端正在运行，软件包刷新或应用状态这样的操作也可能会标示为失败，并显示以下消息：

```
受控端已关闭或无法联系。
```

在此情况下，请尝试重新安排该操作。如果重新安排成功，发生问题的原因可能在于 DNS 配置有误。

Salt 客户端重启动时，或者系统在刷新 grain 时，客户端会计算其 FQDN grain，并在 grain 继续执行前保持无响应状态。当 SUSE Manager Server 上安排的操作将要执行时，SUSE Manager Server 会先于实际操作向客户端发出 `test.ping`，以确保客户端实际上正在运行，可以触发该操作。

默认情况下，SUSE Manager Server 会等待 5 秒来获得 `test.ping` 命令的响应。如果在 5 秒内未收到响应，则会将该操作设置为失败，并显示消息指出客户端已关闭或无法联系。

要解决此问题，请修复客户端上的 DNS 解析，使客户端在解析其 FQDN 时不会卡顿 5 秒时间。

如果无法修复，请尝试将 SUSE Manager Server 上 `/etc/rhn/rhn.conf` 文件中 `java.salt_presence_ping_timeout` 的值增至大于 4 的值。

例如：

```
java.salt_presence_ping_timeout = 6
```

之后，使用以下命令重启动 `spacewalk-services`：

```
spacewalk-services restart
```

> 将此值增大会使 SUSE Manager 服务器花费更长时间检查受控端是否无法连接或无响应，导致 SUSE Manager 服务器总体速度更慢或响应能力更低。

27.38. Saltboot 公式查错

由于计算出的分区大小值有问题，在 SLE 11 SP3 客户端上创建的 Saltboot 公式有时会失败，并出现如下所示的错误：

```
      ID: disk1_partitioned
  Function: saltboot.partitioned
    Name: disk1
   Result: false
  Comment: An exception occurred in this state: Traceback (most recent call last):
 File "/usr/lib/python2.6/site-packages/salt/state.py", line 1767, in call
  **cdata['kwargs'])
 File "/usr/lib/python2.6/site-packages/salt/loader.py", line 1705, in wrapper
  return f(*args, **kwargs)
 File "/var/cache/salt/minion/extmods/states/saltboot.py", line 393, in disk_partitioned
  existing = __salt__['partition.list'](device, unit='MiB')
 File "/usr/lib/python2.6/site-packages/salt/modules/parted.py", line 177, in list_
  'Problem encountered while parsing output from parted')
CommandExecutionError: Problem encountered while parsing output from parted
```

可以通过手动配置包含操作系统的分区大小来解决此问题。正确设置大小后，即可预期方式正常创建公式。

过程：在 Saltboot 公式中手动配置分区大小

1. 在 SUSE Manager Web UI 中，导航到**系统 › 系统组**并选择包含导致错误的 SLE 11 SP3 客户端的硬件类型组。 在公式选项卡中，导航到 `Saltboot` 子选项卡。
2. 找到包含操作系统的分区，然后在分区大小字段中键入适当的大小（以 MiB 为单位）。
3. 单击 **[保存公式]**，然后应用 Highstate 以保存更改。

27.39. 对纲要升级失败的问题进行查错

如果纲要升级失败，数据库版本检查和所有其他 spacewalk 服务都不会启动。请运行 `spacewalk-service start`，获取有关如何继续的详细信息和提示。

您也可以直接运行版本检查：

```
systemctl status uyuni-check-database.service
```

或

```
journalctl -u uyuni-check-database.service
```

如果您不想运行更常规的 `spacewalk-service` 命令，这些命令会列显调试信息。

27.40. 同步查错

同步失败的原因有很多。要获取有关连接问题的详细信息，请运行以下命令：

```
export URLGRABBER_DEBUG=DEBUG
spacewalk-repo-sync -c <通道名称> <选项> > /var/log/spacewalk-repo-sync-$(date +%F-%R).log
2>&1
```

还可以检查 Zypper 在 `/var/log/zypper.log` 处创建的日志

GPG 密钥不匹配

SUSE Manager 不会自动信任第三方 GPG 密钥。如果软件包同步失败，原因可能是某个 GPG 密钥不受信任。您可以通过打开 `/var/log/rhn/reposync` 并查找如下所示的错误来确定这是否是原因所在：

```
['/usr/bin/spacewalk-repo-sync', '--channel', 'sle-12-sp1-ga-desktop-
nvidia-driver-x86_64', '--type', 'yum', '--non-interactive']
RepoMDError：无法访问储存库。可能未导入储存库 GPG 密钥
```

要解决该问题，需要将 GPG 密钥导入 SUSE Manager。有关导入 GPG 密钥的详细信息，请参见 **Administration › Repo-metadata**。

从 `spacewalk-repo-sync` 去除 GPG 密钥

使用 `spacewalk-repo-sync` 手动导入储存库的 GPG 密钥后，如果不再需要此密钥（例如，由于该密钥已泄露或仅用于测试目的），可通过以下命令从 `spacewalk-repo-sync` 使用的 zypper RPM 数据库中去除该密钥：

```
rpm --dbpath=/var/lib/spacewalk/reposync/root/var/lib/rpm/ -e gpg-pubkey-*
```

其中 `gpg-pubkey-*` 是要去除的 GPG 密钥的名称。

续订 GPG 密钥

如果您要续订某个 GPG 密钥，请先去除旧密钥，然后生成并导入新密钥。

校验和不匹配

如果校验和失败，`/var/log/rhn/reposync/*.log` 日志文件中可能会显示如下所示的错误：

```
Repo Sync Errors: (50, u'checksums did not match
326a904c2fbd7a0e20033c87fc84ebba6b24d937 vs
afd8c60d7908b2b0e2d95ad0b333920aea9892eb', 'Invalid information uploaded
to the server')
The package microcode_ctl-1.17-102.57.62.1.x86_64 which is referenced by
patch microcode_ctl-8413 was not found in the database. This patch has
been skipped.
```

可以通过在命令提示符下使用 `-Y` 选项运行同步来解决此错误：

```
spacewalk-repo-sync --channel <通道名称> -Y
```

此选项在同步之前校验储存库数据，而不是依赖于本地缓存的校验和。

连接超时

如果下载超时并出现以下错误：

```
28：操作速度太慢。过去 300 秒的传输速率小于 1000 字节/秒
```

您可以通过在 `/etc/rhn/rhn.conf` 中指定 `reposync_timeout` 和 `reposync_minrate` 配置值来解决此错误。默认情况下，如果在 300 秒内的传输速率小于 1000 字节/秒，则下载将会中止。您可以使用 `reposync_minrate` 调整每秒字节数，并使用 `reposync_timeout` 调整等待的秒数。

27.41. Taskomatic 查错

储存库元数据重新生成是一个资源消耗量相对较高的进程，因此 Taskomatic 可能需要几分钟才能完成。此外，如果 Taskomatic 崩溃，则储存库元数据重新生成可能会中断。

如果 Taskomatic 仍在运行，或者该进程已崩溃，则软件包更新可能在 Web UI 中看似可用，但不会显示在客户端上，并且尝试更新客户端会失败。在这种情况下，`zypper ref` 命令会显示如下所示的错误：

```
在指定的 URL 上找不到有效元数据
```

要更正此问题，请确定 Taskomatic 是否仍在生成储存库元数据，或者是否发生了崩溃。等待完成元数据重新生成，或者在崩溃后重启动 Taskomatic 以正常执行客户端更新。

过程：解决 Taskomatic 问题

1. 在 SUSE Manager Server 上，检查 `/var/log/rhn/rhn_taskomatic_daemon.log` 文件以确定是否有任何元数据重新生成进程仍在运行，或者是否发生了崩溃。
2. 重启动 Taskomatic：

   ```
   service taskomatic restart
   ```

3. 在 Taskomatic 日志文件中，可以通过查看如下所示的开始行和结束行来识别与元数据重新生成相关的部分：

```
<YYYY-DD-MM> <HH:MM:SS>,174 [Thread-584] INFO
com.redhat.rhn.taskomatic.task.repomd.RepositoryWriter - Generating new repository
metadata for channel 'cloned-2018-q1-sles12-sp3-updates-x86_64'(sha256) 550 packages,
140 errata

...

<YYYY-DD-MM> <HH:MM:SS>,704 [Thread-584] INFO
com.redhat.rhn.taskomatic.task.repomd.RepositoryWriter - Repository metadata generation
for 'cloned-2018-q1-sles12-sp3-updates-x86_64' finished in 4 seconds
```

27.42. 对 Web UI 无法加载的问题进行查错

有时，Web UI 在迁移后不会加载。如果新系统的主机名和 IP 地址与旧系统的相同，这种情况通常是由浏览器缓存所致。两个系统的主机名和 IP 地址相同可能会使一些浏览器产生混淆。

清除缓存并重新加载页面可以解决此问题。在大多数浏览器中，可通过按 `Ctrl` ⌧+⌧ `F5` 快速解决此问题。

Chapter 28. GNU Free Documentation License

Copyright © 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document' s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document' s license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License.