



U Y U N I

Uyuni 2024.07

客户端配置指南

2024年07月 4日



目录

客户端配置指南概述	1
1. 支持的客户端和功能	2
1.1. 支持的客户端系统	2
1.2. 支持的工具软件包	3
1.3. Supported SLES and openSUSE Features	3
1.4. Supported SLE Micro Features	5
1.5. 支持的 SL Micro 客户端功能	7
1.6. openSUSE Leap Micro Client Features	9
1.7. 支持的 Alibaba Cloud Linux 功能	11
1.8. 支持的 AlmaLinux 功能	13
1.9. 支持的 Amazon Linux 功能	15
1.10. 支持的 CentOS 功能	17
1.11. 支持的 Debian 功能	19
1.12. Supported openEuler Features	21
1.13. 支持的 Oracle 功能	23
1.14. Supported Raspberry Pi OS Features	25
1.15. 支持的 Red Hat Enterprise Linux 功能	27
1.16. 支持的 Rocky Linux 功能	29
1.17. 支持的 Ubuntu 功能	31
2. 配置基本知识	34
2.1. 软件通道	34
2.1.1. 通过 SUSE Package Hub 提供的软件包	34
2.1.2. 通过 AppStream 提供的软件包	35
2.1.3. 通过 EPEL 提供的软件包	35
2.1.4. SUSE Linux Enterprise 客户端的 Unified Installer 更新通道	35
2.1.5. 软件储存库	35
2.1.6. 软件产品	36
2.1.7. AppStream Modules	37
2.2. 引导储存库	37
2.2.1. 准备创建引导储存库	37
2.2.2. 自动模式的选项	38
2.2.3. 手动生成引导储存库	38
2.2.4. 引导和自定义通道	40
2.3. 激活密钥	40
2.3.1. 重新激活密钥	42
2.3.2. 激活密钥最佳实践	42
2.4. GPG 密钥	43
2.4.1. 在客户端上信任 GPG 密钥	44
3. Client Contact Methods	46
3.1. Default Contact Method (Salt)	46
3.1.1. 初始配置细节	47
3.2. SSH Push Contact Method	47
3.2.1. Available parameters	49
3.2.2. 操作的执行	50
3.2.3. Future features	50
3.3. SSH Push (With Tunnel) Contact Method	50
3.4. Salt 捆绑包	52
3.4.1. 什么是 Salt 捆绑包?	53
3.4.2. 使用 Salt 捆绑包将客户端注册为受控端	53
3.4.3. SSH Push with the Salt Bundle	54
3.4.4. 使用 pip 通过 Python 软件包扩展 Salt 捆绑包	55
4. 客户端注册	56

4.1. Registration Methods	56
4.1.1. 使用 Web UI 注册客户端	56
4.1.2. Register Clients with a Bootstrap Script	58
4.1.3. Register Clients on the Command Line	61
4.2. SUSE 客户端注册	63
4.2.1. 注册 SUSE Linux Enterprise 客户端	64
4.2.2. 注册 SLE Micro 客户端	67
4.2.3. 注册 SL Micro 客户端	72
4.3. openSUSE 客户端注册	74
4.3.1. 注册 openSUSE Leap 客户端	75
4.3.2. Registering openSUSE Leap Micro Clients	77
4.4. Alibaba Cloud Linux 客户端注册	79
4.4.1. 注册 Alibaba Cloud Linux 客户端	79
4.5. AlmaLinux 客户端注册	81
4.5.1. 注册 AlmaLinux 客户端	81
4.6. Amazon Linux 客户端注册	83
4.6.1. 注册 Amazon Linux 客户端	83
4.7. CentOS 客户端注册	86
4.7.1. 注册 CentOS 客户端	86
4.8. Debian 客户端注册	90
4.8.1. 注册 Debian 客户端	90
4.9. OpenEuler Client Registration	93
4.9.1. Registering openEuler Clients	93
4.10. Oracle 客户端注册	97
4.10.1. 注册 Oracle Linux 客户端	97
4.11. Raspberry Pi OS Client Registration	99
4.11.1. Registering Raspberry Pi OS Clients	100
4.12. Red Hat 客户端注册	103
4.12.1. 使用 CDN 注册 Red Hat Enterprise Linux 客户端	104
4.12.2. Registering Red Hat Enterprise Linux clients with RHUI	111
4.13. Rocky Linux 客户端注册	116
4.13.1. 注册 Rocky Linux 客户端	116
4.14. Ubuntu 客户端注册	119
4.14.1. 注册 Ubuntu 20.04 和 22.04 客户端	119
4.15. Client Registration to a Proxy	123
4.15.1. Move Clients Between Proxies	124
4.15.2. 将客户端从代理移到服务器	125
4.15.3. 使用 Web UI 将客户端注册到代理	125
4.15.4. Register Clients on the Command Line	125
4.16. Registering Clients on a Public Cloud	126
4.16.1. 添加产品并同步储存库	126
4.16.2. Prepare On-demand Images	126
4.16.3. 注册客户端	127
4.16.4. 激活密钥	127
4.16.5. 自动注册 Terraform 创建的客户端	128
5. 客户端升级	130
5.1. Major Version Upgrade	130
5.1.1. Prepare to Migrate	130
5.1.2. 迁移	132
5.2. 使用内容生命周期管理器升级	133
5.2.1. 准备升级	133
5.2.2. 升级	134
5.3. 产品迁移	135
5.3.1. 单系统迁移	135
5.3.2. 产品大量迁移	136
5.4. 升级 Uyuni 客户端	139

5.4.1. 准备升级	139
5.4.2. 升级	140
6. 客户端删除	141
6.1. 使用 Web UI 删除客户端	141
6.2. Delete a Client on the Command Line (with API Call)	141
6.3. 从命令行删除客户端	142
7. 客户端操作	143
7.1. 软件包管理	143
7.1.1. 校验软件包	143
7.1.2. 比较软件包	143
7.2. 补丁管理	144
7.2.1. 创建补丁	144
7.2.2. 将补丁应用到客户端	145
7.3. 系统锁定	146
7.3.1. System Locks on Clients	146
7.3.2. 软件包锁	147
7.4. 配置管理	148
7.4.1. 创建配置通道	148
7.4.2. 添加配置文件、目录或符号链接	149
7.4.3. 为客户端订阅配置通道	150
7.4.4. 比较配置文件	150
7.4.5. Jinja templating on clients	150
7.5. 电源管理	151
7.5.1. 电源管理和 Cobbler	151
7.6. 自定义系统信息	152
7.7. 系统集管理器	152
7.7.1. 在 SSM 中更改基础通道	154
7.8. 系统组	154
7.8.1. 创建组	154
7.8.2. 将客户端添加到组	155
7.8.3. 使用组	155
7.9. 系统类型	156
8. 操作系统安装	157
8.1. 重新安装已注册系统	157
8.2. 通过 CD-ROM 或 USB 密钥安装	158
8.2.1. 使用 Cobbler 构建 ISO 映像	158
8.2.2. 使用 KIWI 构建 SUSE ISO 映像	159
8.2.3. 使用 Cobbler 构建 Red Hat ISO 映像	159
8.3. 可自动安装的发行套件	159
8.3.1. 基于 ISO 映像的发行套件	160
8.3.2. 基于 RPM 软件包的发行套件	160
8.3.3. 声明可自动安装的发行套件	161
8.4. 自动安装配置文件	162
8.4.1. 声明配置文件	162
8.4.2. AutoYaST 配置文件	163
8.4.3. Kickstart Profiles	164
8.4.4. Templates Syntax	164
8.5. 无人照管的置备	166
8.6. 使用您自己的 GPG 密钥	167
8.6.1. 用于 PXE 引导的自己的 GPG 密钥	167
8.6.2. Own GPG Key in a CD-ROM	168
9. 虚拟化	169
9.1. Manage Virtualized Hosts	169
9.2. 创建虚拟 Guest	169
9.3. 使用 Xen 和 KVM 虚拟化	170

9.3.1. 主机设置	170
9.3.2. 自动安装 VM Guest	171
9.3.3. 管理 VM Guest	175
10. 虚拟主机管理器	176
10.1. Virtual Host Manager and Amazon Web Services	176
10.1.1. 创建 Amazon EC2 VHM	176
10.1.2. 虚拟主机管理器的 AWS 权限	177
10.2. Virtual Host Manager and Azure	177
10.2.1. 先决条件	178
10.2.2. 创建 Azure VHM	178
10.2.3. 指派权限	178
10.2.4. Azure UUID	179
10.3. Virtual Host Manager and Google Compute Engine	179
10.3.1. 先决条件	179
10.3.2. 创建 GCE VHM	179
10.3.3. 指派权限	180
10.3.4. GCE UUID	181
10.4. 使用 Nutanix 虚拟化	181
10.4.1. VHM 设置	181
10.5. 使用 VMWare 虚拟化	182
10.5.1. VHM 设置	182
10.5.2. 在 VMWare 上对 SSL 错误进行查错	183
10.6. 使用其他第三方提供者虚拟化	184
11. GNU Free Documentation License	186

客户端配置指南概述

更新日期：2024-07-04

安装 Uyuni 后首先要做的就是注册客户端，您花在 Uyuni 上的大部分时间都是用来维护这些客户端。

Uyuni is compatible with SUSE Linux Enterprise or another Linux operating system and with a range of hardware options.

有关支持的客户端和功能的完整列表，请参见 [Client-configuration > Supported-features](#)。

本指南介绍了如何注册以及配置不同的客户端，包括手动和自动两种方式。

Chapter 1. 支持的客户端和功能

Uyuni is compatible with a range of client technologies. You can install Salt clients running SUSE Linux Enterprise or another Linux operating system, with a range of hardware options.

本章提供了支持的客户端系统摘要。有关每个客户端上可用功能的详细列表，请参见后面的页面。

1.1. 支持的客户端系统

Supported operating systems for Salt clients are listed in this table.

此表中图标的含意如下：

- ✓ 运行此操作系统的客户端受 SUSE 支持
- ✗ 运行此操作系统的客户端不受 SUSE 支持
- ? 客户端正在考虑之中，日后可能受支持，也可能不受支持。



客户端操作系统的版本和 SP 级别必须享受标准支持（常规或 LTSS）才受 Uyuni 的支持。有关受支持产品版本的细节，请参见 <https://www.suse.com/lifecycle>。



客户端上运行的操作系统由提供操作系统的组织支持。

表格 1. Supported Client Systems and Architectures

Operating System	x86-64	ppc64le	IBM Z	aarch64	arm64 / armhf
SUSE Linux Enterprise 15, 12	✓	✓	✓	✓	✗
SUSE Linux Enterprise Server for SAP 15, 12	✓	✓	✗	✗	✗
SLE Micro	✓	✗	✗	✓	✗
SL Micro	✓	✗	✗	✓	✗
openSUSE Leap Micro	✓	✗	✗	✓	✗
openSUSE Leap 15	✓	✗	✗	✓	✗
Alibaba Cloud Linux 2	✓	✗	✗	✓	✗
AlmaLinux 9, 8	✓	✗	✗	✓	✗
Amazon Linux 2003, 2	✓	✗	✗	✓	✗
CentOS 7	✓	✓	✗	✓	✗
Debian 12, 11	✓	✗	✗	✗	✗
openEuler 22.03	✓	✗	✗	✗	✗
Oracle Linux 9, 8, 7	✓	✗	✗	✓	✗
Raspberry Pi OS 12	✗	✗	✗	✗	✓

Operating System	x86-64	ppc64le	IBM Z	aarch64	arm64 / armhf
Red Hat Enterprise Linux 9, 8, 7	✓	✗	✗	✗	✗
Rocky Linux 9, 8	✓	✗	✗	✓	✗
Ubuntu 22.04, 20.04	✓	✗	✗	✗	✗



(*) Debian and Ubuntu list the x86-64 architecture as amd64.

发行套件到达生命周期结束日期时，将进入 3 个月的宽限期，届时支持将视为处于弃用状态。宽限期结束之后，产品即视为不受支持。此后我们将只能尽最大努力提供支持。

有关生命周期结束日期的详细信息，请参见 <https://endoflife.software/operating-systems>。

1.2. 支持的工具软件包

spacewalk-utils 和 spacewalk-utils-extras 软件包可提供额外的服务和功能。

表格 2. Spacewalk 实用程序

工具名称	说明	受支持?
spacewalk-common-channels	添加 SUSE Customer Center 不提供的通道	✓
spacewalk-hostname-rename	更改 Uyuni 服务器的主机名	✓
spacewalk-clone-by-date	按特定日期克隆通道	✓
spacewalk-sync-setup	设置 ISS 主组织和从属组织映射	✓
spacewalk-manage-channel-lifecycle	管理通道生命周期	✓

1.3. Supported SLES and openSUSE Features

下表列出了 SUSE 和 openSUSE 客户端上各种功能的可用性。该表涵盖了 SUSE Linux Enterprise 操作系统的所有变体，包括 SLES、SLED、SUSE Linux Enterprise Server for SAP 和 SUSE Linux Enterprise Server for HPC。



客户端上运行的操作系统由提供操作系统的组织支持。SUSE Linux Enterprise 由 SUSE 支持。openSUSE 由 SUSE 社区支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 3. SUSE 和 openSUSE 操作系统上支持的功能

Feature	SUSE Linux Enterprise 12	SUSE Linux Enterprise 15	openSUSE 15
Client	✓	✓	✓
System packages	SUSE	SUSE	openSUSE Community
Registration	✓	✓	✓
Install packages	✓	✓	✓
Apply patches	✓	✓	✓
Remote commands	✓	✓	✓
System package states	✓	✓	✓
System custom states	✓	✓	✓
Group custom states	✓	✓	✓
Organization custom states	✓	✓	✓
System set manager (SSM)	✓	✓	✓
Product migration	✓	✓	✓
Basic Virtual Guest Management *	✓	✓	✓
Advanced Virtual Guest Management *	✓	✓	✓
Virtual Guest Installation (AutoYaST), as Host OS	✗	✗	✗
Virtual Guest Installation (image template), as Host OS	✓	✓	✓
Virtual Guest Management	✓	✓	✓
System deployment (PXE/AutoYaST)	✓	✓	✓
System redeployment (AutoYaST)	✓	✓	✓
Contact methods	✗	✗	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓	✓
Action chains	✓	✓	✓
Staging (pre-download of packages)	✓	✓	✓
Duplicate package reporting	✓	✓	✓

Feature	SUSE Linux Enterprise 12	SUSE Linux Enterprise 15	openSUSE 15
CVE auditing	✓	✓	✓
SCAP auditing	✓	✓	✓
Package verification	✗	✗	✗
Package locking	✓	✓	✓
System locking	✗	✗	✗
Maintenance Windows	✓	✓	✓
System snapshot	✗	✗	✗
Configuration file management	✓	✓	✓
Package profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓	✓
Monitoring server	✓	✓	✓
Monitored clients	✓	✓	✓
Docker buildhost	✓	✓	?
Build Docker image with OS	✓	✓	✓
Kiwi buildhost	✓	?	?
Build Kiwi image with OS	✓	?	✗
Recurring Actions	✓	✓	✓
AppStreams	N/A	N/A	N/A
Yomi	✗	✓	✓

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.4. Supported SLE Micro Features



客户端上运行的操作系统由提供操作系统的组织支持。SLE Micro 由 SUSE 支持。



目前，SLE Micro 仅支持作为常规的受控端（----联系方法）。我们正在努力实现也将其作为 Salt SSH 客户端（salt-ssh 联系方法）的功能。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 4. SLE Micro 操作系统上支持的功能

Feature	SLE Micro
Client	✓
Operating system packages	✓
Registration	✓
Install packages	✓
Apply patches (requires CVE ID)	✓
Remote commands	✓
System package states	✓
System custom states	✓
Group custom states	✓
Organization custom states	✓
System set manager (SSM)	✓
Product migration	✓
Basic Virtual Guest Management *	✓
Advanced Virtual Guest Management *	✓
Virtual Guest Installation (Kickstart), as Host OS	✓
Virtual Guest Installation (image template), as Host OS	✓
System deployment (PXE/Kickstart)	✓
System redeployment (Kickstart)	✓
Contact methods	✓ ZeroMQ
Works with Uyuni Proxy	✓
Action chains	✓
Staging (pre-download of packages)	?
Duplicate package reporting	✓
CVE auditing (requires CVE ID)	✓

Feature	SLE Micro
SCAP auditing	?
Package verification	?
Package locking	✓
System locking	?
Maintenance Windows	?
System snapshot	✗
Configuration file management	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported
Power management	✓
Monitoring server	✗
Monitored clients **	✓
Docker buildhost	✗
Build Docker image with OS	✗
Kiwi buildhost	✗
Build Kiwi image with OS	✓
Recurring Actions	✓
AppStreams	N/A
Yomi	?

****** 虚拟 Guest 管理:

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

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

1.5. 支持的 SL Micro 客户端功能



客户端上运行的操作系统由提供操作系统的组织支持。SL Micro 由 SUSE 支持。



目前 SL Micro 仅支持作为使用----联系方法的 Salt 客户端。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 5. SLE Micro 操作系统上支持的功能

Feature	SLE Micro
Client	Salt
Operating system packages	Salt
Registration	Salt
Install packages	Salt
Apply patches (requires CVE ID)	Salt
Remote commands	Salt
System package states	Salt
System custom states	Salt
Group custom states	Salt
Organization custom states	Salt
System set manager (SSM)	Salt
Product migration	Salt
Basic Virtual Guest Management *	?
Advanced Virtual Guest Management *	?
Virtual Guest Installation (Kickstart), as Host OS	✗
Virtual Guest Installation (image template), as Host OS	?
System deployment (PXE/Kickstart)	?
System redeployment (Kickstart)	✗
Contact methods	Salt: ZeroMQ
Works with Uyuni Proxy	Salt
Action chains	Salt
Staging (pre-download of packages)	?
Duplicate package reporting	Salt
CVE auditing (requires CVE ID)	Salt
SCAP auditing	?
Package verification	?
Package locking	Salt
System locking	?
Maintenance Windows	?

Feature	SLE Micro
System snapshot	✗
Configuration file management	Salt
Snapshots and profiles	Salt: Profiles supported, Sync not supported
Power management	Salt
Monitoring server	✗
Monitored clients **	Salt
Docker buildhost	✗
Build Docker image with OS	✗
Kiwi buildhost	✗
Build Kiwi image with OS	Salt
Recurring Actions	Salt
AppStreams	N/A
Yomi	?

***** 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

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

1.6. openSUSE Leap Micro Client Features



openSUSE Leap Micro is supported by the SUSE community.

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 6. Supported Features on openSUSE Leap Micro Operating Systems

Feature	openSUSE Leap Micro
Client	✓

Feature	openSUSE Leap Micro
Operating system packages	✓
Registration	✓
Install packages	✓
Apply patches (requires CVE ID)	✓
Remote commands	✓
System package states	✓
System custom states	✓
Group custom states	✓
Organization custom states	✓
System set manager (SSM)	✓
Product migration	✓
Basic Virtual Guest Management *	✓
Advanced Virtual Guest Management *	✓
Virtual Guest Installation (Kickstart), as Host OS	✓
Virtual Guest Installation (image template), as Host OS	✓
System deployment (PXE/Kickstart)	✓
System redeployment (Kickstart)	✓
Contact methods	✓ ZeroMQ
Works with Uyuni Proxy	✓
Action chains	✓
Staging (pre-download of packages)	?
Duplicate package reporting	✓
CVE auditing (requires CVE ID)	✓
SCAP auditing	?
Package verification	?
Package locking	✓
System locking	?
Maintenance Windows	?
System snapshot	✗
Configuration file management	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported
Power management	✓

Feature	openSUSE Leap Micro
Monitoring server	✗
Monitored clients	✓
Docker buildhost	✗
Build Docker image with OS	✗
Kiwi buildhost	✗
Build Kiwi image with OS	✓
Recurring Actions	✓
AppStreams	N/A
Yomi	?

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.7. 支持的 Alibaba Cloud Linux 功能

下表列出了 Alibaba Cloud Linux 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。Alibaba Cloud Linux 由 Alibaba Cloud 支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 7. Alibaba Cloud Linux 操作系统上支持的功能

Feature	Alibaba Cloud Linux 2
Client	✓
Operating system packages	✓
Registration	✓
Install packages	✓

Feature	Alibaba Cloud Linux 2
Apply patches (requires CVE ID)	✓
Remote commands	✓
System package states	✓
System custom states	✓
Group custom states	✓
Organization custom states	✓
System set manager (SSM)	✓
Product migration	N/A
Basic Virtual Guest Management *	?
Advanced Virtual Guest Management *	?
Virtual Guest Installation (Kickstart), as Host OS	✗
Virtual Guest Installation (image template), as Host OS	?
System deployment (PXE/Kickstart)	?
System redeployment (Kickstart)	?
Contact methods	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓
Action chains	✓
Staging (pre-download of packages)	✓
Duplicate package reporting	✓
CVE auditing (requires CVE ID)	✓
SCAP auditing	✓
Package verification	✗
Package locking	✗
System locking	✗
Maintenance Windows	✓
System snapshot	✗
Configuration file management	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported
Power management	?
Monitoring server	✗
Monitored clients	✓
Docker buildhost	✓

Feature	Alibaba Cloud Linux 2
Build Docker image with OS	✓
Kiwi buildhost	✓
Build Kiwi image with OS	✓
Recurring Actions	✓
AppStreams	N/A
Yomi	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.8. 支持的 AlmaLinux 功能

下表列出了 AlmaLinux 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。AlmaLinux 由 AlmaLinux 社区支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 8. AlmaLinux 操作系统上支持的功能

Feature	AlmaLinux 9	AlmaLinux 8
Client	✓ (plain AlmaLinux)	✓ (plain AlmaLinux)
System packages	AlmaLinux Community	AlmaLinux Community
Registration	✓	✓
Install packages	✓	✓
Apply patches	✓	✓
Remote commands	✓	✓
System package states	✓	✓

Feature	AlmaLinux 9	AlmaLinux 8
System custom states	✓	✓
Group custom states	✓	✓
Organization custom states	✓	✓
System set manager (SSM)	✓	✓
Product migration	N/A	N/A
Basic Virtual Guest Management *	✓	✓
Advanced Virtual Guest Management *	✓	✓
Virtual Guest Installation (Kickstart), as Host OS	✗	✗
Virtual Guest Installation (image template), as Host OS	✓	✓
System deployment (PXE/Kickstart)	✓	✓
System redeployment (Kickstart)	✓	✓
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓
Action chains	✓	✓
Staging (pre-download of packages)	✓	✓
Duplicate package reporting	✓	✓
CVE auditing	✓	✓
SCAP auditing	✓	✓
Package verification	✗	✗
Package locking	✗	✗
System locking	✗	✗
Maintenance Windows	✓	✓
System snapshot	✗	✗
Configuration file management	✓	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓
Monitoring server	✗	✗
Monitored clients	✓	✓

Feature	AlmaLinux 9	AlmaLinux 8
Docker buildhost	✗	✗
Build Docker image with OS	✗	✗
Kiwi buildhost	✗	✗
Build Kiwi image with OS	✗	✗
Recurring Actions	✓	✓
AppStreams	✓	✓
Yomi	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.9. 支持的 Amazon Linux 功能

下表列出了 Amazon Linux 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。Amazon Linux 由 Amazon 支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 9. Amazon Linux 操作系统上支持的功能

Feature	Amazon Linux 2	Amazon Linux 2023
Client	✓	✓
Operating system packages	✓	✓
Registration	✓	✓
Install packages	✓	✓
Apply patches (requires CVE ID)	✓	✓
Remote commands	✓	✓

Feature	Amazon Linux 2	Amazon Linux 2023
System package states	✓	✓
System custom states	✓	✓
Group custom states	✓	✓
Organization custom states	✓	✓
System set manager (SSM)	✓	✓
Product migration	N/A	N/A
Basic Virtual Guest Management *	?	?
Advanced Virtual Guest Management *	?	?
Virtual Guest Installation (Kickstart), as Host OS	✗	✗
Virtual Guest Installation (image template), as Host OS	?	?
System deployment (PXE/Kickstart)	?	?
System redeployment (Kickstart)	?	?
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓
Action chains	✓	✓
Staging (pre-download of packages)	✓	✓
Duplicate package reporting	✓	✓
CVE auditing (requires CVE ID)	✓	✓
SCAP auditing	✓	✓
Package verification	✗	✗
Package locking	✗	✗
System locking	✗	✗
Maintenance Windows	✓	✓
System snapshot	✗	✗
Configuration file management	✓	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	?	?
Monitoring server	✗	✗

Feature	Amazon Linux 2	Amazon Linux 2023
Monitored clients	✓	✓
Docker buildhost	✓	✓
Build Docker image with OS	✓	✓
Kiwi buildhost	✓	✓
Build Kiwi image with OS	✓	✓
Recurring Actions	✓	✓
AppStreams	N/A	N/A
Yomi	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.10. 支持的 CentOS 功能

下表列出了 CentOS 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。CentOS 由 CentOS 社区支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 10. CentOS 操作系统上支持的功能

Feature	CentOS 7
Client	✓ (plain CentOS)
System packages	CentOS Community
Registration	✓
Install packages	✓
Apply patches (requires CVE ID)	✓ (third-party service required for errata)

Feature	CentOS 7
Remote commands	✓
System package states	✓
System custom states	✓
Group custom states	✓
Organization custom states	✓
System set manager (SSM)	✓
Product migration	N/A
Basic Virtual Guest Management *	✓
Advanced Virtual Guest Management *	✓
Virtual Guest Installation (Kickstart), as Host OS	✗
Virtual Guest Installation (image template), as Host OS	✓
System deployment (PXE/Kickstart)	✓
System redeployment (Kickstart)	✓
Contact methods	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓
Action chains	✓
Staging (pre-download of packages)	✓
Duplicate package reporting	✓
CVE auditing (requires CVE ID)	✓
SCAP auditing	✓
Package verification	✗
Package locking	✓
System locking	✗
Maintenance Windows	✓
System snapshot	✗
Configuration file management	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported
Power management	✓
Monitoring server	✗
Monitored clients	✓
Docker buildhost	✗
Build Docker image with OS	✗

Feature	CentOS 7
Kiwi buildhost	✗
Build Kiwi image with OS	✗
Recurring Actions	✓
AppStreams	N/A
Yomi	N/A

* 虚拟 Guest 管理:

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.11. 支持的 Debian 功能

下表列出了 Debian 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。Debian 由 Debian 社区支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 11. Debian 操作系统上支持的功能

Feature	Debian 11	Debian 12
Client	✓	✓
System packages	Debian Community	Debian Community
Registration	✓	✓
Install packages	✓	✓
Apply patches	?	?
Remote commands	✓	✓
System package states	✓	✓
System custom states	✓	✓

Feature	Debian 11	Debian 12
Group custom states	✓	✓
Organization custom states	✓	✓
System set manager (SSM)	✓	✓
Product migration	N/A	N/A
Basic Virtual Guest Management *	✓	✓
Advanced Virtual Guest Management *	✓	✓
Virtual Guest Installation (Kickstart), as Host OS	✓	✓
Virtual Guest Installation (image template), as Host OS	✓	✓
System deployment (PXE/Kickstart)	✓	✓
System redeployment (Kickstart)	✗	✗
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓
Action chains	✓	✓
Staging (pre-download of packages)	✓	✓
Duplicate package reporting	✓	✓
CVE auditing	?	?
SCAP auditing	?	?
Package verification	✗	✗
Package locking	✓	✓
System locking	✗	✗
Maintenance Windows	✓	✓
System snapshot	✗	✗
Configuration file management	✓	✓
Package profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓
Monitoring server	✗	✗
Monitoring clients	✓	✓
Docker buildhost	?	?

Feature	Debian 11	Debian 12
Build Docker image with OS	Salt	Salt
Kiwi buildhost	✗	✗
Build Kiwi image with OS	✗	✗
Recurring Actions	✓	✓
AppStreams	N/A	N/A
Yomi	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.12. Supported openEuler Features

This table lists the availability of various features on openEuler clients.



The operating system you run on a client is supported by the organization that supplies the operating system. openEuler is supported by the openEuler community.

此表中图标的含意如下：

- ✓ the feature is available on both Salt
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 12. Supported Features on openEuler Operating Systems

Feature	openEuler 22.03
Client	✓ (plain openEuler)
System packages	openEuler Community
Registration	✓
Install packages	✓
Apply patches	✓
Remote commands	✓
System package states	✓

Feature	openEuler 22.03
System custom states	✓
Group custom states	✓
Organization custom states	✓
System set manager (SSM)	✓
Product migration	N/A
Basic Virtual Guest Management *	✓
Advanced Virtual Guest Management *	✓
Virtual Guest Installation (Kickstart), as Host OS	✗
Virtual Guest Installation (image template), as Host OS	✓
System deployment (PXE/Kickstart)	✓
System redeployment (Kickstart)	✓
Contact methods	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓
Action chains	✓
Staging (pre-download of packages)	✓
Duplicate package reporting	✓
CVE auditing	✓
SCAP auditing	✓
Package verification	✗
Package locking	✗
System locking	✗
Maintenance Windows	✓
System snapshot	✗
Configuration file management	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported
Power management	✓
Monitoring	✓
Docker buildhost	✗
Build Docker image with OS	✗
Kiwi buildhost	✗
Build Kiwi image with OS	✗
Recurring Actions	✓

Feature	openEuler 22.03
Yomi	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.13. 支持的 Oracle 功能

下表列出了 Oracle Linux 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。Oracle Linux 由 Oracle 支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✘ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 13. Oracle Linux 操作系统上支持的功能

Feature	Oracle Linux 7	Oracle Linux 8	Oracle Linux 9
Client	✓	✓	✓
Operating system packages	✓	✓	✓
Registration	✓	✓	✓
Install packages	✓	✓	✓
Apply patches (requires CVE ID)	✓	✓	✓
Remote commands	✓	✓	✓
System package states	✓	✓	✓
System custom states	✓	✓	✓
Group custom states	✓	✓	✓
Organization custom states	✓	✓	✓

Feature	Oracle Linux 7	Oracle Linux 8	Oracle Linux 9
System set manager (SSM)	✓	✓	✓
Product migration	N/A	N/A	N/A
Basic Virtual Guest Management *	✓	✓	✓
Advanced Virtual Guest Management *	✓	✓	✓
Virtual Guest Installation (Kickstart), as Host OS	✗	✓	✓
Virtual Guest Installation (image template), as Host OS	✓	✓	✓
System deployment (PXE/Kickstart)	✓	✓	✓
System redeployment (Kickstart)	✓	✓	✓
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓	✓
Action chains	✓	✓	✓
Staging (pre-download of packages)	✓	✓	✓
Duplicate package reporting	✓	✓	✓
CVE auditing (requires CVE ID)	✓	✓	✓
SCAP auditing	✓	✓	✓
Package verification	✗	✗	✗
Package locking	✓	✓	✓
System locking	✗	✗	✗
Maintenance Windows	✓	✓	✓
System snapshot	✗	✗	✗
Configuration file management	✓	✓	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓	✓
Monitoring server	✗	✗	✗
Monitored clients	✓	✓	✓

Feature	Oracle Linux 7	Oracle Linux 8	Oracle Linux 9
Docker buildhost	✗	✗	✗
Build Docker image with OS	✗	✗	✗
Kiwi buildhost	✗	✗	✗
Build Kiwi image with OS	✗	✗	✗
Recurring Actions	✓	✓	✓
AppStreams	N/A	✓	✓
Yomi	N/A	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.14. Supported Raspberry Pi OS Features

This table lists the availability of various features on Raspberry Pi OS clients.



The operating system you run on a client is supported by the organization that supplies the operating system. Raspberry Pi OS is supported by the Raspberry Pi OS community.

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 14. Supported Features on Raspberry Pi OS Operating Systems

Feature	Raspberry Pi OS 12
Client	✓
System packages	Raspberry Pi OS Community
Registration	✓
Install packages	✓
Apply patches	?

Feature	Raspberry Pi OS 12
Remote commands	✓
System package states	✓
System custom states	✓
Group custom states	✓
Organization custom states	✓
System set manager (SSM)	✓
Product migration	N/A
Basic Virtual Guest Management *	✓
Advanced Virtual Guest Management *	✓
Virtual Guest Installation (Kickstart), as Host OS	✗
Virtual Guest Installation (image template), as Host OS	✓
System deployment (PXE/Kickstart)	✗
System redeployment (Kickstart)	✗
Contact methods	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓
Action chains	✓
Staging (pre-download of packages)	✓
Duplicate package reporting	✓
CVE auditing	?
SCAP auditing	?
Package verification	✗
Package locking	✓
System locking	✗
Maintenance Windows	✓
System snapshot	✗
Configuration file management	✓
Package profiles	✓ Profiles supported, Sync not supported
Power management	✓
Monitoring server	✗
Monitoring clients	✓
Docker buildhost	?
Build Docker image with OS	✓

Feature	Raspberry Pi OS 12
Kiwi buildhost	✗
Build Kiwi image with OS	✗
Recurring Actions	✓
AppStreams	N/A
Yomi	N/A

* 虚拟 Guest 管理:

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.15. 支持的 Red Hat Enterprise Linux 功能

This table lists the availability of various features on native Red Hat Enterprise Linux clients.



- 客户端上运行的操作系统由提供操作系统的组织支持。Red Hat Enterprise Linux 由 Red Hat 支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 15. Red Hat Enterprise Linux 操作系统上支持的功能

Feature	RHEL 7	RHEL 8	RHEL 9
Client	✓	✓	✓
System packages	Red Hat	Red Hat	Red Hat
Registration	✓	✓	✓
Install packages	✓	✓	✓
Apply patches	✓	✓	✓
Remote commands	✓	✓	✓
System package states	✓	✓	✓
System custom states	✓	✓	✓

Feature	RHEL 7	RHEL 8	RHEL 9
Group custom states	✓	✓	✓
Organization custom states	✓	✓	✓
System set manager (SSM)	✓	✓	✓
Product migration	N/A	N/A	N/A
Basic Virtual Guest Management *	✓	✓	✓
Advanced Virtual Guest Management *	✓	✓	✓
Virtual Guest Installation (Kickstart), as Host OS	✗	✗	✗
Virtual Guest Installation (image template), as Host OS	✓	✓	✓
System deployment (PXE/Kickstart)	✓	✓	✓
System redeployment (Kickstart)	✓	✓	✓
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓	✓
Action chains	✓	✓	✓
Staging (pre-download of packages)	✓	✓	✓
Duplicate package reporting	✓	✓	✓
CVE auditing	✓	✓	✓
SCAP auditing	✓	✓	✓
Package verification	✗	✗	✗
Package locking	✓	✓	✓
System locking	✗	✗	✗
Maintenance Windows	✓	✓	✓
System snapshot	✗	✗	✗
Configuration file management	✓	✓	✓
Snapshots and profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓	✓

Feature	RHEL 7	RHEL 8	RHEL 9
Monitoring server	✗	✗	✗
Monitored clients	✓	✓	✓
Docker buildhost	✓	✓	✓
Build Docker image with OS	?	?	?
Kiwi buildhost	✗	✗	✗
Build Kiwi image with OS	✗	✗	✗
Recurring Actions	✓	✓	✓
AppStreams	N/A	✓	✓
Yomi	N/A	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.16. 支持的 Rocky Linux 功能

下表列出了 Rocky Linux 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织提供支持。Rocky Linux 由 Debian 社区提供支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 16. Rocky Linux 操作系统上支持的功能

Feature	Rocky Linux 8	Rocky Linux 9
Client	✓ (plain Rocky Linux)	✓ (plain Rocky Linux)
System packages	Rocky Linux Community	Rocky Linux Community
Registration	✓	✓

Feature	Rocky Linux 8	Rocky Linux 9
Install packages	✓	✓
Apply patches	✓	✓
Remote commands	✓	✓
System package states	✓	✓
System custom states	✓	✓
Group custom states	✓	✓
Organization custom states	✓	✓
System set manager (SSM)	✓	✓
Product migration	N/A	N/A
Basic Virtual Guest Management *	✓	✓
Advanced Virtual Guest Management *	✓	✓
Virtual Guest Installation (Kickstart), as Host OS	✗	✗
Virtual Guest Installation (image template), as Host OS	✓	✓
System deployment (PXE/Kickstart)	✓	✓
System redeployment (Kickstart)	✓	✓
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓
Action chains	✓	✓
Staging (pre-download of packages)	✓	✓
Duplicate package reporting	✓	✓
CVE auditing	✓	✓
SCAP auditing	✓	✓
Package verification	✗	✗
Package locking	✓	✓
System locking	✗	✗
Maintenance Windows	✓	✓
System snapshot	✗	✗
Configuration file management	✓	✓

Feature	Rocky Linux 8	Rocky Linux 9
Snapshots and profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓
Monitoring server	✗	✗
Monitored clients	✓	✓
Docker buildhost	✗	✗
Build Docker image with OS	✗	✗
Kiwi buildhost	✗	✗
Build Kiwi image with OS	✗	✗
Recurring Actions	✓	✓
AppStreams	✓	✓
Yomi	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

1.17. 支持的 Ubuntu 功能

下表列出了 Ubuntu 客户端上各种功能的可用性。



客户端上运行的操作系统由提供操作系统的组织支持。Ubuntu 由 Canonical 支持。

此表中图标的含意如下：

- ✓ the feature is available
- ✗ 该功能不可用
- ? 该功能正在考虑之中，日后可能提供，也可能不提供

表格 17. Ubuntu 操作系统上支持的功能

Feature	Ubuntu 20.04	Ubuntu 22.04
Client	✓	✓
System packages	Canonical	Canonical

Feature	Ubuntu 20.04	Ubuntu 22.04
Registration	✓	✓
Install packages	✓	✓
Apply patches	✓	✓
Remote commands	✓	✓
System package states	✓	✓
System custom states	✓	✓
Group custom states	✓	✓
Organization custom states	✓	✓
System set manager (SSM)	✓	✓
Product migration	N/A	N/A
Basic Virtual Guest Management *	✓	✓
Advanced Virtual Guest Management *	✓	✓
Virtual Guest Installation (Kickstart), as Host OS	✗	✗
Virtual Guest Installation (image template), as Host OS	✓	✓
System deployment (PXE/Kickstart)	✗	✗
System redeployment (Kickstart)	✗	✗
Contact methods	✓ ZeroMQ, Salt-SSH	✓ ZeroMQ, Salt-SSH
Works with Uyuni Proxy	✓	✓
Action chains	✓	✓
Staging (pre-download of packages)	✓	✓
Duplicate package reporting	✓	✓
CVE auditing	?	?
SCAP auditing	?	?
Package verification	✗	✗
Package locking	✓	✓
System locking	✗	✗
System snapshot	✗	✗
Configuration file management	✓	✓

Feature	Ubuntu 20.04	Ubuntu 22.04
Package profiles	✓ Profiles supported, Sync not supported	✓ Profiles supported, Sync not supported
Power management	✓	✓
Monitoring	✓	✓
Docker buildhost	?	?
Build Docker image with OS	✓	✓
Kiwi buildhost	✗	✗
Build Kiwi image with OS	✗	✗
Recurring Actions	✓	✓
AppStreams	N/A	N/A
Yomi	N/A	N/A

* 虚拟 Guest 管理：

在此表格中，虚拟 Guest 管理分为基本管理和高级管理。

基本虚拟 Guest 管理包括列出 VM、慢速刷新、VM 生命周期操作（开始、停止、继续、暂停）以及修改 VM vCPU 和内存。

高级虚拟 Guest 管理包括基本虚拟 Guest 管理的所有功能以及快速刷新、VM 生命周期操作（删除、重置、关机）、修改 VM 磁盘、网络、图形显示和图形显示配置。

Chapter 2. 配置基本知识

Uyuni 需要您执行一些步骤来准备客户端注册环境，然后才能使用该环境的各项操作。

本章总结了在成功安装和设置 Uyuni 后为支持环境操作而必须执行的初始配置步骤。

- 有关安装 Uyuni 的详细信息，请参见 [Installation-and-upgrade > Install-uyuni](#)。
- 有关设置 Uyuni 的详细信息，请参见 [Installation-and-upgrade > Uyuni-server-setup](#)。

2.1. 软件通道

通道是一种用于对软件包分组的方法。软件包由储存库提供，而储存库与通道关联。客户端订阅软件通道后，便可安装并更新与其关联的任何软件。

在 Uyuni 中，通道分为基础通道和子通道。以此方式组织通道可确保每个系统上只安装兼容的软件包。客户端只能订阅一个基础通道，该通道是在注册期间根据客户端操作系统和体系结构指派的。对于供应商提供的付费通道，您必须具有关联的订阅。

基础通道中包含为特定操作系统类型、版本和体系结构构建的软件包。例如，SUSE Linux Enterprise Server 15 x86-64 基础通道中仅包含与该操作系统和体系结构兼容的软件。

子通道与基础通道关联，仅提供与基础通道兼容的软件包。一个系统可订阅其基础通道的多个子通道。将系统指派到基础通道后，该系统便只能安装相关的子通道。例如，如果将系统指派到 SUSE Linux Enterprise Server 15 x86_64 基础通道，那么便只能安装或更新通过兼容基础通道或它的任何关联子通道提供的软件包。

在 Uyuni Web UI 中，您可以导航到 [软件 > 通道列表 > 所有](#) 来浏览可用通道。您可以通过导航到 [软件 > 管理 > 通道修改](#) 或 [创建新通道](#)。

有关使用通道（包括自定义通道）的详细信息，请参见 [Administration > Channel-management](#)。

2.1.1. 通过 SUSE Package Hub 提供的软件包

SUSE Package Hub 是 SUSE Linux Enterprise 产品的扩展，用于提供额外的开源软件（由 openSUSE 社区提供）。



SUSE Package Hub 中的软件包由 openSUSE 社区提供。SUSE 不会为这些软件包提供支持。

如果您在客户端上使用的是 SUSE Linux Enterprise 操作系统，则可启用 SUSE Package Hub 扩展来访问这些额外的软件包。这样会提供 SUSE Package Hub 通道，您可以为客户端订阅这些通道。

SUSE Package Hub 提供了大量软件包，可能需要花很长时间进行同步，并会占用大量磁盘空间。除非您确实需要 SUSE Package Hub 提供的软件包，否则请不要启用它。

为了避免无意间安装或更新不支持的软件包，建议您实施一开始会拒绝所有 SUSE Package Hub 软件包的内容生命周期管理策略。然后，您可以显式启用所需的特定软件包。有关内容生命周期管理的详细信息，请参见

Administration > Content-lifecycle。

2.1.2. 通过 AppStream 提供的软件包

对于基于 Red Hat 的客户端，通过 AppStream 来提供额外的软件包。大多数情况下都需要 AppStream 软件包来确保您已拥有所有必需的软件。

2.1.3. 通过 EPEL 提供的软件包

对于基于 Red Hat 的客户端，通过 EPEL 提供额外的软件包（适用于企业版 Linux 的额外软件包）。EPEL 是可选软件包储存库，用于提供额外的软件。



EPEL 中的软件包由 Fedora 社区提供。SUSE 不会为这些软件包提供支持。

如果您在客户端上使用的是 Red Hat 操作系统，则可启用 EPEL 扩展来访问这些额外的软件包。这样会提供 EPEL 通道，您可以为客户端订阅这些通道。

EPEL 提供了大量软件包，可能需要花很长时间进行同步，并会占用大量磁盘空间。除非您确实需要 EPEL 提供的软件包，否则请不要启用 EPEL 储存库。

为了避免无意间安装或更新不支持的软件包，建议您实施一开始会拒绝所有 EPEL 软件包的内容生命周期管理 (CLM) 策略。然后，您可以显式启用所需的特定软件包。有关内容生命周期管理的详细信息，请参见 Administration > Content-lifecycle。

2.1.4. SUSE Linux Enterprise 客户端的 Unified Installer 更新通道

Unified Installer 使用此通道来确保其在安装操作系统前是最新的。所有 SUSE Linux Enterprise 产品在安装期间都应能够访问安装程序更新通道。

对于 SUSE Linux Enterprise Server 客户端，默认会在您添加包含安装程序更新通道的产品时对这些通道进行同步，并会在您创建包含这些产品通道的可自动安装发行套件时予以启用。

对于所有其他 SUSE Linux Enterprise 变体，包括 SUSE Linux Enterprise for SAP，您必须手动添加安装程序更新通道。要完成此操作，请克隆这些 SUSE Linux Enterprise 变体的基础通道下的相应 SUSE Linux Enterprise Server 安装程序更新通道。克隆通道后，为这些 SUSE Linux Enterprise 变体创建可自动安装的发行套件时，会自动使用相应通道。

2.1.5. 软件储存库

储存库用于收集软件包。如果您有权访问软件储存库，便可以安装储存库提供的任何软件。在 Uyuni 中，必须至少有一个储存库与您的软件通道相关联，才能向该通道指派客户端并在客户端上安装和更新软件包。

Uyuni 中的大多数默认通道都已与正确的储存库关联。如果您要创建自定义通道，则需要关联您有权访问的或您自己创建的储存库。

有关自定义储存库和通道的详细信息，请参见 Administration > Custom-channels。

2.1.5.1. 本地储存库位置

You can configure local repositories on clients, to provide packages that are not supplied by Uyuni channels.



大多数情况下，客户端系统不需要本地储存库。本地储存库可能会导致无法确定客户端上哪些软件包可用，而这可能会导致安装非预期的软件包。

初始配置期间会禁用本地储存库。

Local repositories will be disabled each time a channel state is executed. For example, when applying the highstate or performing a package action.

If local repositories should stay enabled after onboarding, the following pillar must be set for the affected client:

编辑 /srv/pillar/top.sls 文件：

```
base:
  'minionid':
    - localrepos
```

编辑 /srv/pillar/localrepos.sls 文件：

```
mgr_disable_local_repos: False
```

客户端完成初始配置后，您可以在以下位置添加本地储存库：

表格 18. 本地储存库位置

Client Operating System	Local Repository Directory
SUSE Linux Enterprise Server	/etc/zypp/repos.d
openSUSE	/etc/zypp/repos.d
Red Hat Enterprise Linux and similar derivatives	/etc/yum.repos.d/
Ubuntu	/etc/apt/sources.list.d/
Debian	/etc/apt/sources.list.d/

2.1.6. 软件产品

在 Uyuni 中，软件通过不同的产品提供。利用 SUSE 订阅，您可以访问各种不同的产品，通过在 Uyuni Web UI 中导航到 **管理 > 安装向导 > 产品** 可以浏览和选择这些产品。

产品包含任意数量的软件通道。单击  图标可查看产品中包含的通道。成功添加并同步产品后，您便可以访问产品提供的通道，并可以在 Uyuni 服务器和客户端上使用产品中的软件包。

过程：添加软件通道

1. 在 Uyuni Web UI 中，导航到管理，安装向导，产品。
2. 使用搜索栏找到适用于您的客户端操作系统和体系结构的产品，然后选中相应产品。这样会自动选中所有必需的通道。此外，建议的所有通道也将选中，并且 开关会打开。单击箭头以查看相关产品的完整列表，确保您需要的所有额外产品都已选中。
3. 单击 并等待产品完成同步。

2.1.7. AppStream Modules

If you are managing a client that is subscribed to an AppStream channel, Uyuni will filter packages available to the client depending on its currently enabled set of AppStream modules.

Procedure: Managing enabled AppStream modules

1. In the Uyuni Web UI, navigate to **Systems > Software > AppStreams**.
2. From the table of module streams, select the streams to be enabled on the client.
3. Click .
4. On the next page, check the list of changes to be made, and choose a time for the action to occur.
5. Click to schedule the changes to be applied.

2.2. 引导储存库

A bootstrap repository contains required packages for registering clients during bootstrapping. When products are synchronized, bootstrap repositories are automatically created and regenerated on the Uyuni Server.

2.2.1. 准备创建引导储存库

如果您选择某个产品以进行同步，当所有必需的通道都完全镜像后，会立即自动创建引导储存库。

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到 选项卡，然后单击 并选中 .

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。 您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

2.2.2. 自动模式的选项

您可以更改自动引导储存库的创建方式。本节介绍了各种相应设置。

刷新模式：

刷新模式

默认只会使用最新软件包更新现有储存库，而您可以将其配置为始终从空储存库开始。要启用此行为，请在 `/etc/rhn/rhn.conf` 中添加或编辑此值：

```
server.susemanager.bootstrap_repo_flush = 1
```

自动模式：

自动模式

默认会启用引导储存库的自动重新生成功能。要禁用此功能，请在 `/etc/rhn/rhn.conf` 中添加或编辑此值：

```
server.susemanager.auto_generate_bootstrap_repo = 0
```

2.2.2.1. 配置引导数据文件

该工具使用包含有关每个发行套件所需软件包的信息的数据文件。该数据文件存储在 `/usr/share/susemanager/mgr_bootstrap_data.py`。SUSE 会定期更新此文件。如果您要更改此文件，请不要直接编辑，而是应在同一目录中创建一份副本，然后编辑该副本：

```
cd /usr/share/susemanager/
cp mgr_bootstrap_data.py my_data.py
```

更改后，将 Uyuni 配置为使用这个新文件。在 `/etc/rhn/rhn.conf` 中添加或编辑此值：

```
server.susemanager.bootstrap_repo_datamodule = my_data
```



下次更新时，SUSE 提供的新数据将重写原来的数据文件，而不是这个新文件。您需要在新文件中使用 SUSE 提供的更改覆盖相应内容，以使其保持最新。

2.2.3. 手动生成引导储存库

默认情况下，每天都会重新生成引导储存库。您可以在命令提示符处手动创建引导储存库。

过程：生成 SUSE Linux Enterprise 的引导储存库

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份列出要为其创建引导储存库的可用发行套件：

```
mgr-create-bootstrap-repo -l
```

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 -c SLE-version-x86_64
```

3. Alternatively, use the number shown next to the distribution name in the list of available distributions.

客户端储存库位于 `/srv/www/htdocs/pub/repositories/` 中。

如果您镜像了多个产品（例如 SLES 和 SLES for SAP），或者您使用的是自定义通道，在创建引导储存库时将需要指定要使用的父通道。并不是在所有情况下都需要如此。例如，部分 SLES 15 版本使用共同的代码库，因此无需指定父通道。只有您的环境需要时，才需使用此过程。

可选过程：指定引导储存库的父通道

1. 检查您有哪些父通道可用：

```
mgr-create-bootstrap-repo -c SLE-15-x86_64
```

找到多个父通道选项。请使用

`--with-parent-channel <label>` 选项并选择以下其中一个父通道：

- `sle-product-sles15-pool-x86_64`
- `sle-product-sles_sap15-pool-x86_64`
- `sle-product-sled15-pool-x86_64`

2. 指定适当的父通道：

```
mgr-create-bootstrap-repo -c SLE-15-x86_64 --with-parent-channel
sle-product-sled15-pool-x86_64
```

2.2.3.1. 包含多个体系结构的储存库

如果您要创建包含多个不同体系结构的引导储存库，则需要确保所有体系结构是否都已正确更新。例如，SLE 的 x86-64 和 IBM Z 体系结构使用相同的引导储存库 URL：`/srv/www/htdocs/pub/repositories/sle/15/2/bootstrap/`。

如果启用 `flush` 选项，当您尝试生成多个体系结构的引导储存库时，将仅生成一个体系结构。要避免此问题，请在创建其他体系结构时于命令提示符处使用 `--no-flush` 选项。例如：

```
mgr-create-bootstrap-repo -c SLE-15-SP2-x86_64  
mgr-create-bootstrap-repo --no-flush -c SLE-15-SP2-s390x
```

2.2.4. 引导和自定义通道

如果您要使用自定义通道，则可以在 `mgr-create-bootstrap-repo` 命令中使用 `--with-custom-channels` 选项。在此情况下，您还需要指定要使用的父通道。

如果您使用自定义通道，则自动创建引导储存库可能会失败。在这种情况下，您需要手动创建储存库。

有关自定义通道的详细信息，请参见 [Administration > Custom-channels](#)。

2.3. 激活密钥

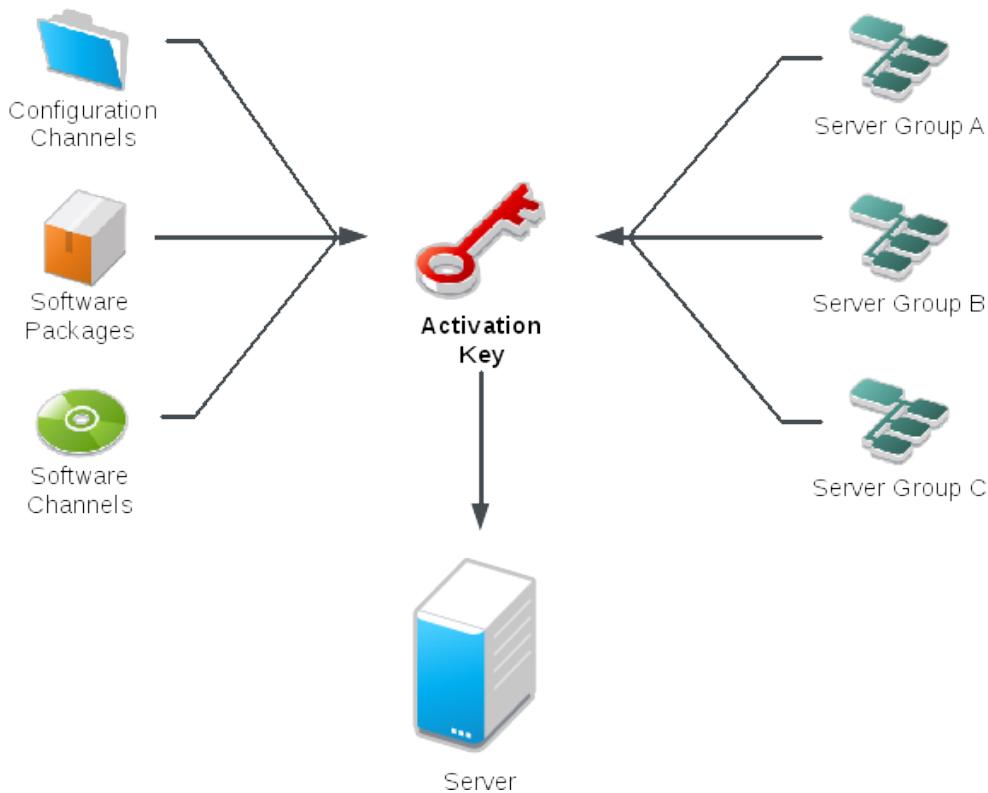
Activation keys are used to ensure that your clients have the correct software entitlements, are connecting to the appropriate channels, and are subscribed to the relevant groups. Each activation key is bound to an organization, which you can set when you create the key.

在 Uyuni 中，激活密钥是一组带有标签的配置设置。您可以通过将某个激活密钥的标签作为参数添加到引导脚本，来应用与该激活密钥关联的所有配置设置。我们建议您结合引导脚本来使用激活密钥标签。当执行引导脚本时，与该标签关联的所有配置设置都将应用到运行脚本的系统上。

激活密钥可以指定以下各项：

- 通道指派
- 系统类型或附加权利
- 联系方法
- 配置文件
- 要安装的软件包
- 系统组

在注册客户端时需使用激活密钥，之后将不再使用。无论激活密钥指定了什么内容，注册好客户端后，就能以任何方式对其进行更改。记录激活密钥与客户端之间的关联仅为了历史记载。



过程：创建激活密钥

1. 在 Uyuni Web UI 中，以管理员身份导航到系统，激活密钥。
2. 单击 **创建密钥** 按钮。
3. 在 **说明** 页面的 **名称** 字段中，输入激活密钥的说明。
4. In the **Key** field, enter a name for the activation key. For example, SLES15-SP5 for SUSE Linux Enterprise Server 15 SP5.



对于任何 SUSE 产品，请不要在 **名称** 字段中使用逗号或双引号。不过，对于 Red Hat 产品，则 **必须** 使用逗号。

- 所有其他字符均可使用，不过系统会自动去除 <> (){}（包括空格）。
- 如果将字段留空，系统会生成一个随机字符串。

5. In the **Base Channels** drop-down box, select the appropriate base software channel, and allow the relevant child channels to populate. For more information, see [reference:admin/setup-wizard.pdf](#) and **Administration > Custom-channels**.
6. 选择所需的子通道（例如，必需的 SUSE Manager 工具和更新通道）。
7. 如果需要启用任何选项，请选中 **启用** 复选框。
8. 建议您保留 **设置** 的 **设置**。
9. 建议您将 **设置** 保留未选中状态。

10. 单击 **[创建激活密钥]** 以创建激活密钥。

11. 选中 **复选框** 以对此密钥启用配置管理，然后单击 **[更新激活密钥]** 保存此更改。



在您创建激活密钥前，**复选框** 将不会显示。如果您需要启用配置管理，请务必返回并选中该复选框。

2.3.1. 重新激活密钥

重新激活密钥可用来重新注册客户端并重新获得所有 Uyuni 设置，但只能使用一次。重新激活密钥为客户端特定密钥，包含系统 ID、历史记录、组和通道。

要创建重新激活密钥，请导航到 **客户端**，单击要为其创建重新激活密钥的客户端，然后导航到 **细节** > **重新激活** 选项卡。单击 **[生成新密钥]** 创建重新激活密钥。记录密钥细节以供日后使用。与未与特定系统关联的典型激活密钥不同，此处创建的密钥不会显示在 **系统** > **激活密钥** 页面中。

After you have created a reactivation key, you can use it as the `management_key` grain in `/etc/salt/minion.d/susemanager.conf`. For example:

```
grains:
  susemanager:
    management_key: "re-1-daf44db90c0853edbb5db03f2b37986e"
```

Restart the `venv-salt-minion` or `salt-minion` process to apply the reactivation key.

您可以结合引导脚本来使用重新激活密钥。有关引导脚本的详细信息，请参见 [Client-configuration](#) > **Registration-bootstrap**。



如果您使用客户端现有的 Uyuni 配置文件自动安装客户端，该配置文件会使用重新激活密钥来重新注册系统并恢复其设置。请勿在正在进行基于配置文件的自动安装时重新生成、删除或使用此密钥，否则会导致自动安装失败。

2.3.2. 激活密钥最佳实践

默认父通道

避免使用 SUSE Manager Default 父通道。此设置会强制 Uyuni 选择与所安装操作系统最匹配的父通道，而这有时可能会导致非预期的行为。请改为创建特定于每个发行套件和体系结构的激活密钥。

使用激活密钥引导

如果要使用引导脚本，请考虑为每个脚本创建一个激活密钥。这有助于您调整通道指派、软件包安装、系统组成员资格和配置通道指派。注册后，您需要与系统手动交互的情形也会减少。

引导 LTSS 客户端

如果要引导订阅了 LTSS 的客户端，请在创建激活密钥期间包含 LTSS 通道。

带宽要求

使用激活密钥可能导致在注册时自动下载软件，这对于存在带宽限制的环境来说可能并不适宜。

下列选择会产生带宽用量：

- 指派 SUSE Product Pool 通道会导致自动安装相应的产品描述符软件包。
- 安装----部分中的所有软件包。
- ----部分中的任何 Salt 状态都可能会触发下载，具体视其内容而定。

密钥标签命名

如果您没有为激活密钥输入直观易懂的名称，系统会自动生成一串数字字符串，这会使得您的密钥难以管理。

请考虑为您的激活密钥使用一种命名模式，以方便您进行跟踪。设计与您组织的基础结构相关的名称有助于您更轻松地执行较复杂的操作。

在创建密钥标签时，请考虑以下提示：

- 操作系统命名（必需）：密钥应始终代表提供的设置所适用的操作系统
- 体系结构命名（建议）：除非您的公司仅在一个体系结构上运行（例如 x86_64），否则最好提供含体系结构类型的标签。
- 服务器类型命名：此服务器的用途是什么？
- 位置命名：服务器位于何处？机房、建筑物或部门？
- 日期命名：维护时段、季度等。
- 自定义命名：哪种命名模式符合您组织的需求？

激活密钥标签名称示例：

```
sles15-sp4-web_server-room_129-x86_64
```

```
sles15-sp4-test_packages-blg_502-room_21-ppc64le
```

包含的通道

在创建激活密钥时，您还需要注意哪些软件通道与其关联。应为密钥指派特定的基础通道，不建议使用默认基础通道。有关详细信息，请在 **Client-configuration > Registration-overview** 中查看您要安装的客户端操作系统。

2.4. GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。

在大多数情况下，您无需调整 GPG 设置即可在您的客户端上安装软件。

可以直接对 RPM 软件包签名，而基于 Debian 的系统仅会对元数据签名并使用校验和链来保障软件包的安全。大多数基于 RPM 的系统除了使用已签名软件包外，还会使用已签名元数据。

2.4.1. 在客户端上信任 GPG 密钥

操作系统要么直接信任自己的 GPG 密钥，要么至少将它们与最小系统一起安装，但通过其他 GPG 密钥签名的第三方软件包需要手动处理。客户端可以在不信任 GPG 密钥的情况下成功引导，但除非密钥受信任，否则您将无法安装新的客户端工具软件包或更新软件包。

Clients now use GPG key information entered for a software channel to manage the trusted keys. When a software channel with GPG key information is assigned to a client, the key is trusted when the channel is refreshed or the first package is installed from this channel.

软件通道页面中的 GPG 密钥 URL 参数可以包含以空格分隔的多个密钥 URL。如果其为文件 URL，则必须在使用软件通道之前在客户端上部署 GPG 密钥文件。

The GPG keys for the Client Tools Channels of Red Hat based clients are deployed on the client into `/etc/pki/rpm-gpg/` and can be referenced with file URLs.

Only in case a software channel is assigned to the client they will be imported and trusted by the system.



由于基于 Debian 的系统仅会对元数据签名，因此不需要为各个通道指定确切的密钥。如果用户按 **Administration > Repo-metadata** 中的“使用自己的 GPG 密钥”所述配置了自己的 GPG 密钥来对元数据签名，系统会自动部署并信任该密钥。

2.4.1.1. 用户定义的 GPG 密钥

Users can define custom GPG keys to be deployed to a client.

通过提供某些 pillar 数据并在 Salt 文件系统中提供 GPG 密钥文件，系统会自动将它们部署到客户端。

这些密钥会分别部署到 `/etc/pki/rpm-gpg/`（在基于 RPM 的操作系统上）和 `/usr/share/keyrings/`（在 Debian 系统上）中：

为你要将密钥部署到的客户端定义 pillar 键 `custom_gpgkeys` 并列出密钥文件名。

```
cat /srv/pillar/mypillar.sls
custom_gpgkeys:
  - my_first_gpg.key
  - my_second_gpgkey.gpg
```

此外，在 Salt 文件系统中创建名为 `gpg` 的目录，并将 `custom_gpgkeys` pillar 数据中所指定的 GPG 密钥文件存储在该目录下。

```
ls -la /srv/salt/gpg/
/srv/salt/gpg/my_first_gpg.key
/srv/salt/gpg/my_second_gpgkey.gpg
```

The keys are deployed to the client at `/etc/pki/rpm-gpg/my_first_gpg.key` and `/etc/pki/rpm-gpg/my_second_gpgkey.gpg`.

最后一步是将 URL 添加到软件通道的“GPG 密钥 URL”字段中。请导航到[软件](#)，[管理](#)，[通道](#)，然后选择要修改的通道。将值 `file:///etc/pki/rpm-gpg/my_first_gpg.key` 添加到 GPG 公钥 URL 中。

2.4.1.2. 引导脚本中的 GPG 密钥

过程：在客户端上使用引导脚本信任 GPG 密钥

1. 在 Uyuni 服务器上的命令提示符处，检查 `/srv/www/htdocs/pub/` 目录的内容。此目录包含所有可用的公共密钥。记下为您正在注册的客户端指派的通道适用的密钥。
2. 打开相关的引导脚本，找到 `ORG_GPG_KEY=` 参数并添加所需的密钥。例如：

```
uyuni-gpg-pubkey-0d20833e.key
```

您无需删除任何以前存储的密钥。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。如果不信任 GPG 密钥，便无法为客户端指派软件通道。

Chapter 3. Client Contact Methods

There are three contact methods how the Uyuni Server can communicate with clients. They are based on Salt protocols.

Which Salt contact method you use depends on the type of client, and your network architecture:

Default (Salt)

is the default choice and is recommended unless there are specific needs. For more information, see [Client-configuration > Contact-methods-default](#).

SSH Push

is useful only if network restrictions make it impossible for clients to establish contact to the server. It is supported with the Salt Bundle only. This contact method has serious limitations. For more information, see [Client-configuration > Contact-methods-saltssh](#).

SSH Push (with tunnel)

is the same as SSH Push, but with using a secured communication tunnel. For more information, see [Client-configuration > Contact-methods-saltssh-tunnel](#).

Implementation of Salt communication software options:

Salt 捆绑包

is a single binary package containing Salt Minion, Python 3, required Python modules, and libraries. Thus the Salt contact method is independent from software installed on the client. Using the Salt Bundle is the default. It is the only supported implementation for the SSH Push or SSH Push (with tunnel) contact method. For more information, see [Client-configuration > Contact-methods-saltbundle](#).

Salt Minion

is Salt software installed on the client system.



The so-called traditional contact protocol is no longer supported with Uyuni 5.0 and later. Before upgrading from Uyuni 4 to 5, any existing traditional clients including the traditional proxies must be migrated to Salt or replaced with Salt proxies.

For more information about migrating traditional Uyuni 4 clients to Salt clients, see <https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html>

3.1. Default Contact Method (Salt)

The default contact method using the Salt protocol is recommended unless there are specific needs. For more information about Salt in general, see [Specialized-guides > Salt](#).

Software updates are generally pushed from the server to the client. Connections are initiated from the

client. This means you must open ports on the server, not on clients. The Salt clients are also known as Salt minions. Uyuni Server installs a daemon on every client.

If you need to use Salt clients in a disconnected setup you can configure SSH Push as a contact method. With this contact method, clients can be located in a firewall-protected zone called a DMZ. For more information about SSH Push, see [Client-configuration > Contact-methods-saltssh](#).

3.1.1. 初始配置细节

Salt has its own database to keep the keys for the minions. This needs to be kept in sync with the Uyuni database. As soon as the key is accepted in Salt, the onboarding process in Uyuni starts.

The onboarding process will look for existing systems in the Uyuni database by searching for the `minion_id` and the `machine_id`. Depending on the outcome, the following scenarios are possible:

- If nothing is found, the new system gets created.
- In case an entry with the `minion_id` or the `machine_id` is found, that system will be migrated to match the new system.
- In case there is a match for both entries, and they are not the same system, the onboarding will be aborted with an error.
- In this case the administrator needs to resolve the conflict by removing at least one of the systems.

3.2. SSH Push Contact Method

SSH Push (`ssh-push`) is used in environments where Salt clients cannot reach the Uyuni Server directly. In this environment, clients are located in a firewall-protected zone called a DMZ. No system within the DMZ is authorized to open a connection to the internal network where the Uyuni Server is located.

SSH Push is also to use if installing a daemon agent on clients is not possible.



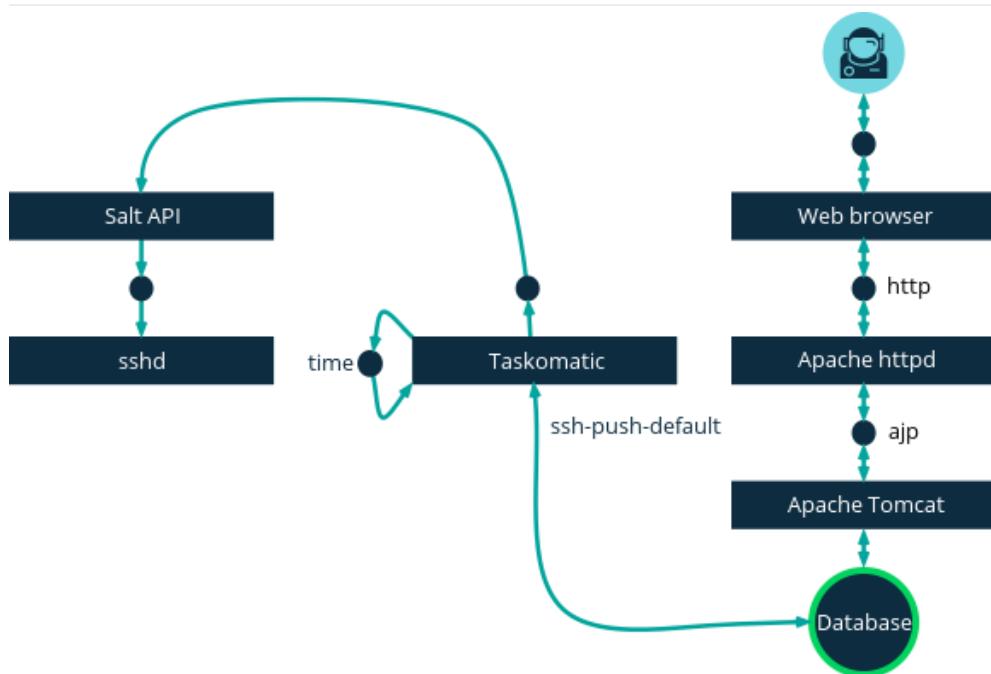
The SSH Push method has serious limitations. It does not scale well, and consumes more Server resources and network bandwidth than the plain Salt method (default). The Push SSH method is not at all supported with large setups (1000 clients and more).

The server uses the SSH Push to contact the clients at regular intervals, checking in and performing scheduled actions and events.



Re-installing systems using the provisioning model is not currently supported on clients managed with SSH Push.

This image demonstrates the SSH Push process path. All items left of the `Taskomatic` block represent processes running on the Uyuni client.



To use SSH Push, you must have the SSH daemon running on the client, and reachable by the `salt-api` daemon running on the Uyuni Server. Additionally, the required Python version will be deployed with the Salt Bundle on the client system.

Before beginning with the following registering procedure, define an activation key with the SSH Push contact method configured. This method expects that there is a direct connection with HTTPS to the Server.

You need to use the Web UI or API to register these clients with the Uyuni Server. See the following procedure or example.

Procedure: Registering clients with SSH Push

1. 在 Uyuni Web UI 中，导航到系统 > 引导，然后填写相应的字段。
2. Select an activation key with the SSH Push contact method configured. For more information about activation keys, see [Client-configuration > Activation-keys](#).
3. 选中 SSH Push 复选框。
4. 单击 **[Bootstrap]** 开始注册。
5. 导航到系统 > 概览，确认该系统已正确注册。

例如：使用 API 访问通过 SSH 推送方法

您可以使用 API 来管理要使用的联系方法。下面的示例 Python 代码将联系方法设为 `ssh-push`。

有效值为：

- default (pull)
- ssh-push
- ssh-push-tunnel

```
client = xmlrpclib.Server(SUMA_HOST + "/rpc/api", verbose=0)
key = client.auth.login(SUMA_LOGIN, SUMA_PASSWORD)
client.system.setDetails(key, 1000012345, {'contact_method' : 'ssh-push'})
```

3.2.1. Available parameters

When you are configuring SSH Push, you can modify parameters that are used when a system is registered, including the host, activation key, and password. The password is used only for bootstrapping, it is not saved anywhere. All future SSH sessions are authorized via a key/certificate pair. These parameters are configured in **Systems > Bootstrapping**.

You can also configure persistent parameters that are used system-wide, including the sudo user to access the system as an unprivileged user instead of as root.

Procedure: Configuring unprivileged SSH access

1. 确保您已在 Uyuni 服务器上安装最新的 spacewalk-taskomatic 和 spacewalk-certs-tools 软件包。
2. 在每个客户端系统上，创建相应的非特权用户。
3. On each client system, edit the sudoers file:

```
sudo visudo
```

4. 在 sudoers 文件末尾添加下面一行，以向用户授予 sudo 访问权限。以在 Web UI 中引导客户端的用户的名称替换 <user>：

```
<user>  ALL=NOPASSWD: /usr/bin/python3, /var/tmp/venv-salt-minion/bin/python
```



此过程无需口令便可授予 root 访问权限，而注册客户端需要提供口令。客户端成功安装后会以 root 特权运行，因此将不再需要该访问权限。客户端成功安装之后，建议您从 sudoers 文件中去除该行。

5. 在 Uyuni 服务器上，于 /etc/rhn/rhn.conf 配置文件中添加或修改下面一行以包含非特权用户名：

```
ssh_push_sudo_user = <user>
```

After changing this configuration parameter you must restart services such as salt-secrets-config.service, tomcat.service, and taskomatic.service. To cover all needed services, it is the best to restart the Uyuni Server as root:

```
mgradm restart
```

3.2.2. 操作的执行

The SSH Push feature uses taskomatic to execute scheduled actions using salt-ssh. The taskomatic job periodically checks for scheduled actions and executes them. The SSH Push feature executes a complete salt-ssh call based on the scheduled action.

默认可以同时执行 20 项 Salt SSH 操作。您可以在配置文件中添加下面几行，并上调 parallel_threads 的值，以增加可同时执行的操作数。建议您将并行操作数设置为较低的值，以免出现问题：

```
taskomatic.sshminion_action_executor.parallel_threads = <number>
org.quartz.threadPool.threadCount = <value of parallel_threads + 20>
```

这样可调整任何客户端上同时运行的操作数，以及 taskomatic 使用的工作器线程总数。如果需要在多个客户端上运行操作，则每个客户端上的操作始终按顺序执行。

如果客户端是通过代理连接的，则需要调整代理上的 MaxSessions 设置。在此情况下，请将并行连接的数量设置为客户端总数的三倍。

3.2.3. Future features

There are some features that are not yet supported on SSH Push. These features do not work on Salt SSH clients:

- OpenSCAP 审计
- 导致以下事件的信标：
 - 使用 zypper 在系统上安装软件包不会调用软件包刷新。
 - 如果虚拟主机系统基于 Salt SSH，则虚拟主机功能（例如 Guest 主机）将无法正常工作。

3.2.3.1. 更多信息

- 有关 Salt SSH 的一般信息，请参见 [Specialized-guides](#) › [Salt](#) 和 <https://docs.saltstack.com/en/latest/topics/ssh/>。
- 有关 SSH 密钥轮替的信息，请参见 [specialized-guides:salt/salt-ssh.pdf](#)。

3.3. SSH Push (With Tunnel) Contact Method

SSH Push (with tunnel) (ssh-push-tunnel) is used in environments where clients cannot reach the Uyuni Server directly. In this environment, clients are located in a firewall-protected zone called a DMZ. No system within the DMZ is authorized to open a connection to the internal network, including the Uyuni Server.

This SSH method creates an encrypted tunnel from the Uyuni Server on the internal network to the clients located on the DMZ. After all actions and events are executed, the tunnel is closed.

服务器使用 SSH 定期联系客户端，以签入和执行安排的操作和事件。



Re-installing systems using the provisioning model is not currently supported on clients managed with SSH Push.



The tunnel is used to provide the access to the server through the encrypted tunnel. The repositories assigned to the SSH Push client (with tunnel) are provided through this tunnel only, thus it is not possible to use package manager tools directly from the client system because the repositories are available only while the tunnel is up. In other words, access is only possible if the session is initiated by the server. All package managing operations on the client can be performed from the server side only.

For tunneling connections via SSH, a port number is required for tunneling via HTTPS. The port number used by default is 1233. To overwrite it, you can add a custom port numbers greater than 1024 to `/etc/rhn/rhn.conf`:

```
ssh_push_port_https = high_port
```

After changing this configuration parameter you must restart services such as `salt-secrets-config.service`, `tomcat.service`, and `taskomatic.service`. To cover all needed services, it is the best to restart `spacewalk-service` as root:

```
spacewalk-service restart
```

出于安全原因，您可能需要结合使用 `sudo` 和 SSH，以非特权用户身份而不是 root 身份访问系统。

过程：配置非特权 SSH 访问

1. 在每个客户端系统上，创建相应的非特权用户。
2. On each client system, edit the `sudoers` file:

```
sudo visudo
```

3. 在 `sudoers` 文件末尾添加下面一行，以向用户授予 `sudo` 访问权限。以在 Web UI 中引导客户端的用户的名称替换 `<user>`：

```
<user>  ALL=NOPASSWD: /usr/bin/python3, /var/tmp/venv-salt-minion/bin/python
```



此过程无需口令便可授予 root 访问权限，而注册客户端需要提供口令。客户端成功安装后会以 root 特权运行，因此将不再需要该访问权限。客户端成功安装之后，建议您从 sudoers 文件中去除该行。

- 在 Uyuni 服务器上，于 /etc/rhn/rhn.conf 配置文件中添加或修改下面一行以包含非特权用户名：

```
ssh_push_sudo_user = <user>
```

After changing this configuration parameter you must restart services such as salt-secrets-config.service, tomcat.service, and taskomatic.service. To cover all needed services, it is the best to restart spacewalk-service as root:

```
spacewalk-service restart
```

You need to use the Web UI or API to register these clients with the Uyuni Server.

Before you begin, you need to ensure that you have specified which ports to use for SSH tunneling. If you have registered clients before changing the port numbers, they need to be registered again with a reactivation key.

- For more information about bootstrapping, see [Client-configuration > Registration-bootstrap](#).
- For more information about bootstrapping, see [client-configuration:activation-keys.pdf](#).

Example: API access to SSH Push (with tunnel)

You can use the API to manage which contact method to use. This example Python code sets the contact method to ssh-push-tunnel.

有效值为：

- default (pull)
- ssh-push
- ssh-push-tunnel

```
client = xmlrpclib.Server(SUMA_HOST + "/rpc/api", verbose=0)
key = client.auth.login(SUMA_LOGIN, SUMA_PASSWORD)
client.system.setDetails(key, 1000012345, {'contact_method' : 'ssh-push-tunnel'})
```

3.4. Salt 捆绑包

3.4.1. 什么是 Salt 捆绑包？

The Salt Bundle is a single binary package containing Salt Minion, Python 3, required Python modules, and libraries.

The Salt Bundle is shipped with Python 3 and all the requirements for Salt to run. Thus Salt Bundle does not use the Python version install on the client as system software. The Salt Bundle can be installed on clients that do not meet the requirements for a given Salt version.

It is also possible to use the Salt Bundle on systems that run a Salt Minion connected to a Salt Master other than the Uyuni Salt Master.

3.4.2. 使用 Salt 捆绑包将客户端注册为受控端

The registration method with the Salt Bundle is the recommended registration method. This section explains the advantages and limitations of the current implementation. The Salt Bundle is provided as the `venv-salt-minion` that consists of Salt, Python 3, and the Python modules Salt depends on. Bootstrapping with Web UI is using Salt Bundle as well, so bootstrapping with Web UI is not Python dependant. Using the Salt Bundle, it is no longer needed that the client provides any Python interpreter or modules.

如果您引导新客户端，默认的注册方法是使用 Salt 捆绑包注册。您可以将现有客户端切换为使用 Salt 捆绑包方法。如果切换，将会安装 `salt-minion` 软件包及其依赖项。

3.4.2.1. Using the Salt Bundle with the Salt Minion

The Salt Bundle can be used with the Salt Minion managed by the Salt Master other than Uyuni Server at the same time. If the Salt Bundle is installed on a client Uyuni Server will manage the configuration files of the Salt Bundle, the configuration files of `salt-minion` will not be managed in this case. For more information, see [Salt Bundle configuration](#).



- To bootstrap a client with the Salt Minion managed by the Salt Master other than Uyuni Server it is recommended to use `mgr-bootstrap --force-bundle` when generating the bootstrap script, or to set `FORCE_VENV_SALT_MINION` to 1 in the bootstrap script.
- 要使用 Web UI 进行引导，可以全局指定 `mgr_force_venv_salt_minion` 设为 `true` 的 pillar。有关详细信息，请参见 [Specialized-guides > Salt](#)。

3.4.2.2. Switching from Salt Minion to Salt Bundle

The Salt state `util.mgr_switch_to_venv_minion` is available to switch from `salt-minion` to `venv-salt-minion`. It is recommended to switch to `venv-salt-minion` in two steps to avoid trouble with shifting processes:

过程：使用 `util.mgr_switch_to_venv_minion` 状态切换到 `venv-salt-minion`

1. 首先，在不指定任何 pillar 的情况下应用 `util.mgr_switch_to_venv_minion`。这样会通过复制配置文件等数据切换到 `venv-salt-minion`。此过程不会清理原始的 `salt-minion` 配置及其软件包。

```
salt <minion_id> state.apply util.mgr_switch_to_venv_minion
```

在 `mgr_purge_non_venv_salt` 设为 `True` (用于去除 `salt-minion`) 以及 `mgr_purge_non_venv_salt_files` 设为 `True` (用于去除与 `salt-minion` 相关的所有文件) 的情况下应用 `util.mgr_switch_to_venv_minion`。此第二步用于确保第一步已经处理，然后去除旧配置文件以及现已过时的 `salt-minion` 软件包。

```
salt <minion_id> state.apply util.mgr_switch_to_venv_minion
pillar='{"mgr_purge_non_venv_salt_files": True,
"mgr_purge_non_venv_salt": True}'
```



如果切换过程中跳过第一步来运行第二步，状态应用过程可能会失败，因为此过程需要停止用于在客户端执行命令的 `salt-minion`。

反过来，您也可以不安装 Salt 捆绑包，而是继续使用 `salt-minion`。在此情况下，请指定以下其中一个选项：

- 指定 `--no-bundle` 选项来执行 `mgr-bootstrap`。
- 在生成的引导脚本中，将 `AVOID_VENV_SALT_MINION` 设为 1。
- 对于引导状态，将 `mgr_avoid_venv_salt_minion` pillar 设为 `True`。

3.4.3. SSH Push with the Salt Bundle

The Salt Bundle is also used when performing SSH Push actions to clients.

A shell script deploys the Salt Bundle onto the target system without installing `venv-salt-minion` before any Salt command is executed. Because the Salt Bundle contains the whole Salt code base, no `salt-thin` is deployed. SSH Push (including bootstrapping using the Web UI) uses the Python 3 interpreter within the bundle. The target system does not need to have any other Python interpreter installed.

The Python 3 deployed with the Bundle is used to handle SSH Push session on the client, so SSH Push (including bootstrapping with Web UI) is not dependant on Python installed on the system.

Using `salt-thin` can be enabled as a fallback method, but it requires Python 3 to be installed on the client. This method is not recommended nor supported and exists for development purposes only. Set `web.ssh_use_salt_thin` to `true` in the `/etc/rhn/rhn.conf` configuration file.

- The bootstrap repository must be created before bootstrapping the client with Web UI. SSH Push is using the Salt Bundle taken from the bootstrap repository based on the detected target operating system. For more information, see [client-configuration:bootstrap-repository.pdf](#).
- SSH Push is using `/var/tmp` to deploy Salt Bundle to and execute Salt commands on the client with the bundled Python. Therefore you must not mount `/var/tmp` with the `noexec` option. It is not possible to bootstrap the clients, which have `/var/tmp` mounted with `noexec` option, with the Web UI because the bootstrap process is using SSH Push to reach a client.

3.4.4. 使用 pip 通过 Python 软件包扩展 Salt 捆绑包

The Salt Bundle includes `pip` to make it possible to extend the functionality of the bundled Salt Minion with extra Python packages.

默认情况下，`salt <minion_id> pip.install <package-name>` 会将 `<package_name>` 指定的 Python 软件包安装到 `/var/lib/venv-salt-minion/local` 中。

 如果需要，可以通过为 `venv-salt-minion.service` 设置 `VENV_PIP_TARGET` 环境变量来覆盖路径 `/var/lib/venv-salt-minion/local`。建议为该服务使用 `systemd` 普适性配置文件。可以使用配置文件 `/etc/systemd/system/venv-salt-minion.service.d/10-pip-destination.conf` 来实现该目的：

```
[Service]
Environment=VENV_PIP_TARGET=/new/path/local/venv-salt-
minion/pip
```

 The Python packages installed through `pip` are not changing on updating the Salt Bundle. To ensure that such packages are available and functional after an update, it is recommended to install them with a Salt state that is applied after Salt Bundle updates.

Chapter 4. 客户端注册

有多种方法可将客户端注册到 Uyuni 服务器。本章介绍了各种可用的方法。此外，还提供了特定于您要在客户端上运行的操作系统的信息。

开始前，请进行以下检查：

- 注册前客户端的日期和时间已与 Uyuni 服务器正确同步。
- 您已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。



Do not register the Uyuni Server base OS to Uyuni itself. The Uyuni Server base OS must be managed individually or by using another separate Uyuni Server.
To manage Uyuni Server Containers, use the `mgradm` tool.

4.1. Registration Methods

有多种方法可将客户端注册到 Uyuni 服务器。

- For only a few clients, we recommend that you register clients using the Uyuni Web UI. 有关详细信息，请参见 [Client-configuration > Registration-webui](#)。
- If you want more control over the process, or have to register many clients, we recommend that you create a bootstrap script. 有关详细信息，请参见 [Client-configuration > Registration-bootstrap](#)。
- For even more control over the process, executing a single commands on the command line can be useful. 有关详细信息，请参见 [Client-configuration > Registration-cli](#)。

注册前，客户端的日期和时间必须已与 Uyuni 服务器正确同步。

您必须先创建激活密钥，然后才能使用引导脚本或命令行方法。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。



Do not register the Uyuni Server to itself. The Uyuni Server must be managed individually or by using another separate Uyuni Server. For more information about using multiple servers, see [Specialized-guides > Large-deployments](#).

4.1.1. 使用 Web UI 注册客户端

Bootstrapping clients with the Web UI is using [Specialized-guides > Salt](#) to execute the bootstrap process on the client. Salt SSH uses the Salt Bundle and its included Python interpreter. Therefore, no other Python interpreter needs to be installed on the client.



由于 Salt 捆绑包通过引导储存库提供，因此在启动客户端的引导过程前，必须创建该储存库。外壳脚本会使用与引导脚本相同的逻辑检测客户端上的操作系统，并部署来自适当引导储存库的 Salt 捆绑包。有关详细信息，请参见[准备创建引导储存库](#)。



Do not register the Uyuni Server to itself. The Uyuni Server must be managed individually or by using another separate Uyuni Server. For more information about using multiple servers, see **Specialized-guides > Large-deployments**.

过程：使用 Web UI 注册客户端

1. 在 Uyuni Web UI 中，导航到**系统 > 引导**。
2. 在**引导 URL**字段中，键入要引导的客户端的完全限定域名 (FQDN)。
3. 在**SSH URL**字段中，键入用于连接和引导客户端的 SSH 端口号。SSH 端口默认为 22。
4. 在**用户名**字段中，键入用于登录客户端的用户名。用户名默认为 root。
5. 要使用 SSH 引导客户端，请在**SSH 私用密钥**字段中选中**SSH 私用密钥**，并上载用于登录客户端的 SSH 私用密钥。如果您的 SSH 私用密钥需要通行口令，请在**SSH 通行口令**字段中键入通行口令。如果不需要，则将该字段留空。
6. 要使用口令引导客户端，请在**口令**字段中选中**口令**，并键入用于登录客户端的口令。
7. 在**激活密钥**字段中，选择与您要用于引导客户端的软件通道关联的激活密钥。有关详细信息，请参见**Client-configuration > Activation-keys**。
8. 可选：在**代理**字段中，选择要将客户端注册到的代理。
9. 默认会选中**自动接受 SSH 主机密钥**复选框。如此可让引导过程自动接受 SSH 主机密钥，而无需您手动进行身份验证。
10. 可选：选中**使用 SSH 来连接服务器**复选框。如果您选中此选项，客户端将会配置为使用 SSH 来连接服务器，且不再配置其他连接方法。
11. 单击**[Bootstrap]**开始注册。

引导过程完成时，您的客户端即会列在**系统 > 系统列表**中。



SSH 私用密钥仅在引导过程期间存储，引导完成后，将会立即从 Uyuni 服务器删除。



使用 Uyuni 在客户端上安装新的软件包或更新时，会自动接受所有最终用户许可协议 (EULA)。要查看软件包 EULA，请打开 Web UI 中的软件包细节页面。

4.1.1.1. Handling of Locally Assigned Repositories

直接将储存库指派给客户端而不通过 Uyuni 提供这种使用情形不常见。这样可能会导致出现问题。因此通过 Salt 引导会在引导过程开始时禁用所有本地储存库。

以后在每次使用通道状态时（例如执行 Highstate 或软件包安装时），所有本地指派的储存库会再次禁用。

客户端上使用的所有软件包均应来自 Uyuni 提供的通道。有关如何创建自定义通道的详细信息，请参见 **Administration > Custom-channels** 中的 [如何操作](#)。

4.1.2. Register Clients with a Bootstrap Script

Registering clients with a bootstrap script gives you control over parameters, and can help if you have to register a large number of clients at once.

To register clients using a bootstrap script, we recommend you create a template bootstrap script to begin, which can then be copied and modified. The bootstrap script you create is executed on the client when it is registered, and ensures all the necessary packages are deployed to the client. Some parameters in the bootstrap script ensure the client system can be assigned to its base channel, using activation key and GPG key.

请务必仔细检查储存库信息，以确保其与基础通道储存库匹配。如果储存库信息未完全匹配，引导脚本将无法下载正确的软件包。



All clients need a bootstrap repository. It is automatically created and regenerated on the Uyuni Server when products are synchronized. A bootstrap repository includes packages for installing Salt on clients, and for registering clients.

For more information about creating a bootstrap repository, see [Client-configuration > Bootstrap-repository](#).



GPG 密钥和 Uyuni 客户端工具

Uyuni 客户端工具使用的 GPG 密钥默认不受信任。创建引导脚本时，请使用 `ORG_GPG_KEY` 参数添加包含公共密钥指纹的文件的路径。



openSUSE Leap 15 和 SLE 15 默认使用 Python 3。必须为 openSUSE Leap 15 和 SLE 15 系统创建基于 Python 2 的引导脚本。如果您使用 Python 2 注册 Leap 15 或 SLE 15 系统，引导脚本将会失败。

4.1.2.1. Create a Bootstrap Script with `mgr-bootstrap`

`mgr-bootstrap` 命令会生成自定义引导脚本。Uyuni 客户端系统可使用引导脚本简化其初始注册和配置流程。

The arguments `--activation-keys` and `--script`, are the only mandatory arguments. On the Uyuni Server, as root at the command line execute it with the mandatory arguments. Replace `<ACTIVATION_KEY>` and `<EDITED_NAME>` with your values:

```
mgr-bootstrap --activation-keys=<ACTIVATION_KEY> --script=bootstrap
-<EDITED_NAME>.sh
```

The `mgr-bootstrap` command offers several other options, including the ability to set a specific

hostname, set specific GPG keys, and set the registration method (salt-minion or salt-bundle).

有关详细信息, 请参见 `mgr-bootstrap` 手册页或运行 `mgr-bootstrap --help`。

4.1.2.2. Create a Bootstrap Script from Web UI

您可以使用 Uyuni Web UI 创建可编辑的引导脚本。

过程: 创建引导脚本

1. 在 Uyuni Web UI 中, 导航到管理, 管理器配置, 引导脚本。
2. 必填字段中会预填充从之前的安装步骤获得的值。有关每个设置的细节, 请参见 **Reference > Admin**。
3. 单击 **[更新]** 创建脚本。
4. 服务器上的 `/srv/www/htdocs/pub/bootstrap` 目录中即会生成并存储引导脚本。或者, 您也可以通过 HTTPS 访问引导脚本。请将 `<example.com>` 替换为您的 Uyuni 服务器的主机名:

```
https://<example.com>/pub/bootstrap/bootstrap.sh
```



请勿在引导脚本中禁用 SSL。请在 Web UI 中确保 `--ssl` 处于选中状态, 或者引导脚本中包含 `USING_SSL=1` 设置。如果您禁用 SSL, 将需要在注册过程中提供自定义 SSL 证书。

For more information about custom certificates, see **Administration > Ssl-certs**.

4.1.2.3. Edit a Bootstrap Script

您可以复制和修改所创建的模板引导脚本, 以对其进行自定义。要将引导脚本用于 Uyuni, 对其进行修改时至少需包含激活密钥。大多数软件包都是使用 GPG 签名的, 因此系统上还需要有可信的 GPG 密钥才能安装这些软件包。

在执行此过程时, 您需要知道激活密钥的确切名称。导航到 **首页** > **概览**, 然后在 `Activation Keys` 框中, 单击 `Activation Keys`。此页面上会列出为通道创建的所有密钥。您在引导脚本中输入的要使用的密钥完整名称必须与密钥字段中显示的名称完全相同。有关激活密钥的详细信息, 请参见 **Client-configuration > Activation-keys**。

过程: 修改引导脚本

1. 在 Uyuni 服务器上的命令行中, 以 root 身份运行以下命令切换到引导目录:

```
cd /srv/www/htdocs/pub/bootstrap/
```

2. 创建并重命名用于每个客户端的两个模板引导脚本副本。

```
cp bootstrap.sh bootstrap-sles12.sh
cp bootstrap.sh bootstrap-sles15.sh
```

3. 打开 `bootstrap-sles15.sh` 进行修改。向下滚动，直到看到如下所示的文本。如果文件中包含 `exit 1`，请在该行的开头键入井号 (#) 将其注释掉。这样会激活脚本。在 `ACTIVATION_KEYS=` 字段中，输入此脚本的密钥的名称：

```
echo "Enable this script: comment (with #'s) this block (or, at
least just"
echo "the exit below)"
echo
#exit 1

# can be edited, but probably correct (unless created during initial
install):
# NOTE: ACTIVATION_KEYS *must* be used to bootstrap a client
machine.
ACTIVATION_KEYS=1-sles15
ORG_GPG_KEY=
```

4. 完成后，保存该文件，然后对第二个引导脚本重复此过程。



By default, bootstrap script will try to install `venv-salt-minion` if it is available in the bootstrap repository and `salt-minion` if there is no Salt bundle in the bootstrap repository. It is possible to avoid installing Salt bundle and keep using `salt-minion` if you need it for some reason.

有关详细信息，请参见 [Client-configuration > Contact-methods-saltbundle](#)。

4.1.2.4. Register Clients Running the Bootstrap Script

创建好脚本后，您便可以使用它来注册客户端。

过程：运行引导脚本

1. On the Uyuni Server, log in as root. At the command prompt, and change to the bootstrap directory:

```
cd /srv/www/htdocs/pub/bootstrap/
```

2. 运行以下命令在客户端上执行引导脚本（将 `EXAMPLE.COM` 替换为客户端的主机名）：

```
cat bootstrap-sles15.sh | ssh root@EXAMPLE.COM /bin/bash
```

3. 或者，在客户端上运行以下命令：

```
curl -Sks https://server_hostname/pub/bootstrap/bootstrap-sles15.sh  
| /bin/bash
```



为避免出现问题，请确保引导脚本是使用 bash 执行的。

此脚本会下载位于您先前创建的储存库目录下的所需依赖项。

4. When the script has finished running, you can check that the client is registered correctly. Open the Uyuni Web UI and navigate to **Systems** > **Overview** to ensure the new client is listed. If the client is not listed, in the Uyuni Web UI navigate to **Salt** > **Keys** and check whether the client key is accepted.



使用 Uyuni 在客户端上安装新的软件包或更新时，会自动接受所有最终用户许可协议 (EULA)。要查看软件包 EULA，请打开 Web UI 中的软件包细节页面。

4.1.3. Register Clients on the Command Line

4.1.3.1. Manual Client Registration

在大多数情况下，使用默认的引导方法即可正确注册 Salt 客户端。不过，您也可以在客户端上编辑 Salt 受控端文件，并提供服务器的完全限定域名 (FQDN)，使用 Salt 手动将客户端注册到 Uyuni 服务器。此方法使用传入服务器的端口 4505 和 4506 来进行。除了需确保这些端口处于打开状态之外，此方法无需在 Uyuni 服务器上进行任何配置。

要执行此过程，您需要在注册前于 Salt 客户端上安装 `venv-salt-minion` (Salt 捆绑包) 或 `salt-minion` 软件包。两种安装会使用位于不同位置但文件名相同的配置文件。`systemd` 服务文件名不同。



只有在您使用属于客户端工具通道或正式 SUSE 发行套件一部分的 `salt-minion` 时，才能以这种方式引导。

4.1.3.2. Salt Bundle Configuration

Salt Bundle (`venv-salt-minion`)

- `/etc/venv-salt-minion/`
- `/etc/venv-salt-minion/minion`
- `/etc/venv-salt-minion/minion.d/NAME.conf`
- `systemd` 服务文件：`venv-salt-minion.service`

有关 Salt 捆绑包的详细信息，请参见 [Client-configuration > Contact-methods-saltbundle](#)。

过程：使用 Salt 捆绑包配置文件注册客户端

- 在 Salt 客户端上，打开 `minion` 配置文件。配置文件位于以下位置：

```
/etc/venv-salt-minion/minion
```

或：

```
/etc/venv-salt-minion/minion.d/NAME.conf
```

- 在文件中添加或编辑 Uyuni 服务器或代理的 FQDN 以及激活密钥（如果有）。另外请添加以下其他配置参数。

```
master: SERVER.EXAMPLE.COM

grains:
  susemanager:
    activation_key: "<Activation_Key_Name>"

  server_id_use_crc: adler32
  enable_legacy_startup_events: False
  enable_fqdns_grains: False
```

- 重启动 `venv-salt-minion` 服务：

```
systemctl restart venv-salt-minion
```

- 在 Uyuni 服务器上，接受新客户端密钥（将 `<client>` 替换为您客户端的名称）：

```
salt-key -a '<client>'
```

4.1.3.3. Client Configuration

Client (`salt-minion`)

- `/etc/salt/`
- `/etc/salt/minion`
- `/etc/salt/minion.d/NAME.conf`
- `systemd` 服务文件：`salt-minion.service`

过程：使用 Salt 受控端配置文件注册客户端

- 在 Salt 客户端上，打开 minion 配置文件。配置文件位于以下位置：

```
/etc/salt/minion
```

或：

```
/etc/salt/minion.d/NAME.conf
```

- In the file add or edit the FQDN of the Uyuni Server or Proxy, and the activation key if any. Also add the other configuration parameters listed below.

```
master: SERVER.EXAMPLE.COM

grains:
  susemanager:
    activation_key: "<Activation_Key_Name>"

server_id_use_crc: adler32
enable_legacy_startup_events: False
enable_fqdns_grains: False
```

- 重启动 salt-minion 服务：

```
systemctl restart salt-minion
```

- 在 Uyuni 服务器上，接受新客户端密钥（将 <client> 替换为您客户端的名称）：

```
salt-key -a '<client>'
```

有关 Salt 受控端配置文件的详细信息，请参见 <https://docs.saltstack.com/en/latest/ref/configuration/minion.html>。

4.2. SUSE 客户端注册

You can register SUSE Linux Enterprise clients to your Uyuni Server.

The method and details varies depending on the operating system of the client.

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。



Do not register a Uyuni Server to itself. The Uyuni Server must be managed individually or by using another separate Uyuni Server. For more information about using multiple servers, see [Specialized-guides > Large-deployments](#).

4.2.1. 注册 SUSE Linux Enterprise 客户端

This section contains information about registering clients running SUSE Linux Enterprise operating systems.

请按照本章中的说明准备所有 SUSE Linux Enterprise 产品，包括：

- SUSE Linux Enterprise Server for SAP
- SUSE Linux Enterprise Desktop
- SUSE Linux Enterprise
- SUSE Linux Enterprise Real Time

您也可以按照这些说明准备较旧的 SUSE Linux Enterprise 版本和服务包。

4.2.1.1. 添加软件通道



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

将 SUSE Linux Enterprise 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

此过程所需的产品包括：

表格 19. SLE 产品 - WebUI

OS Version	Product Name
SUSE Linux Enterprise Server 15 SP6	SUSE Linux Enterprise Server 15 SP6 x86_64
SUSE Linux Enterprise Server 15 SP5	SUSE Linux Enterprise Server 15 SP5 x86_64
SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP4 x86_64
SUSE Linux Enterprise Server 15 SP3	SUSE Linux Enterprise Server 15 SP3 x86_64
SUSE Linux Enterprise Server 15 SP2	SUSE Linux Enterprise Server 15 SP2 x86_64
SUSE Linux Enterprise Server 15 SP1	SUSE Linux Enterprise Server 15 SP1 x86_64
SUSE Linux Enterprise Server 12 SP5	SUSE Linux Enterprise Server 12 SP5 x86_64

过程：添加软件通道

1. 在 Uyuni Web UI 中，导航到管理 > 安装向导 > 产品。
2. 使用搜索栏找到适用于您的客户端操作系统和体系结构的产品，然后选中相应产品。这样会自动选中所有必需的通道。此外，建议的所有通道也将选中，并且 开关会打开。单击箭头以查看相关产品的完整列表，确保您需要的所有额外产品都已选中。
3. 单击  并等待产品完成同步。

或者，您也可以在命令提示符处添加通道。此过程所需的通道包括：

表格 20. SLE 产品 - CLI

OS Version	Base Channel
SUSE Linux Enterprise Server 15 SP6	sle-product-sles15-sp6-pool-x86_64
SUSE Linux Enterprise Server 15 SP5	sle-product-sles15-sp5-pool-x86_64
SUSE Linux Enterprise Server 15 SP4	sle-product-sles15-sp4-pool-x86_64
SUSE Linux Enterprise Server 15 SP3	sle-product-sles15-sp3-pool-x86_64
SUSE Linux Enterprise Server 15 SP2	sle-product-sles15-sp2-pool-x86_64
SUSE Linux Enterprise Server 15 SP1	sle-product-sles15-sp1-pool-x86_64
SUSE Linux Enterprise Server 12 SP5	sle-product-sles15-sp5-pool-x86_64

要查找较旧产品的通道名称，请在 Uyuni 服务器上的命令提示符处以 root 身份使用 `mgr-sync` 命令：

```
mgr-sync list --help
```

然后指定您感兴趣的参数，例如 `channels`：

```
mgr-sync list channels [-c]
```

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `mgr-sync` 命令添加相应的通道：

```
mgr-sync add channel <channel_label_1>
mgr-sync add channel <channel_label_2>
mgr-sync add channel <channel_label_n>
```

2. 同步会自动启动。如果您要手动同步通道，请使用以下命令：

```
mgr-sync sync --with-children <channel_name>
```

3. 确保同步已完成，然后再继续操作。

要添加客户端工具，请在命令提示符处添加以下通道：

表格 21. SUSE Linux Enterprise 通道 - CLI

OS Version	Client Channel
SUSE Linux Enterprise Server 15 SP6	sles15-sp6-uyuni-client
SUSE Linux Enterprise Server 15 SP5	sles15-sp5-uyuni-client
SUSE Linux Enterprise Server 15 SP4	sles15-sp4-uyuni-client
SUSE Linux Enterprise Server 15 SP3	sles15-sp3-uyuni-client
SUSE Linux Enterprise Server 15 SP2	sles15-sp2-uyuni-client
SUSE Linux Enterprise Server 15 SP1	sles15-sp1-uyuni-client
SUSE Linux Enterprise Server 12 SP5	sles12-sp5-uyuni-client

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。

4.2.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到 **同步** 选项卡，然后单击 **同步** 并选中 **正在同步**。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `tail` 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



SUSE Linux Enterprise 通道可能会非常大。同步所需的时间可能会长达数小时。

4.2.1.3. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。



为 SUSE Linux Enterprise Server 15 和 SUSE Linux Enterprise Server 12 客户端使用相同的 GPG 密钥。正确的密钥名为 `sle12-gpg-pubkey-39db7c82.key`。

4.2.1.4. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.2.2. 注册 SLE Micro 客户端

This section contains information about registering clients running SLE Micro operating systems 5.1, 5.2, 5.3, 5.4, and 5.5 on x86-64, arm64, and IBM Z (s390x) architectures.

SLE Micro 是一个超级可靠的轻量级操作系统，专为边缘计算而构建。它利用了 SUSE Linux Enterprise 的强化安全性和合规组件，并将它们整合到一个对开发人员友好的现代化、不可变操作系统平台。

SLE Micro 使用事务更新。事务更新是原子更新（仅当所有更新都成功时，才应用所有更新）且支持回滚。它们不会影响正在运行的系统，因为在系统重引导之前，它们不会激活任何更改。此信息显示在[系统 > 细节 > 概览](#)选项卡中。

有关事务更新和重引导的详细信息，请访问 <https://documentation.suse.com/sles/html/SLES-all/cha-transactional-updates.html>。

4.2.2.1. 添加软件通道

将 SLE Micro 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的产品包括：

表格 22. SLE Micro 产品 - WebUI

操作系统版本	产品名称
SLE Micro 5.5 x86-64	SUSE Linux Enterprise Micro 5.5 x86_64
SLE Micro 5.5 arm64	SUSE Linux Enterprise Micro 5.5 aarch64
SLE Micro 5.5 s390x	SUSE Linux Enterprise Micro 5.5 s390x
SLE Micro 5.4 x86-64	SUSE Linux Enterprise Micro 5.4 x86_64
SLE Micro 5.4 arm64	SUSE Linux Enterprise Micro 5.4 aarch64
SLE Micro 5.4 s390x	SUSE Linux Enterprise Micro 5.4 s390x
SLE Micro 5.3 x86-64	SUSE Linux Enterprise Micro 5.3 x86_64
SLE Micro 5.3 arm64	SUSE Linux Enterprise Micro 5.3 aarch64
SLE Micro 5.3 s390x	SUSE Linux Enterprise Micro 5.3 s390x
SLE Micro 5.2 x86-64	SUSE Linux Enterprise Micro 5.2 x86_64
SLE Micro 5.2 arm64	SUSE Linux Enterprise Micro 5.2 aarch64
SLE Micro 5.2 s390x	SUSE Linux Enterprise Micro 5.2 s390x
SLE Micro 5.1 x86-64	SUSE Linux Enterprise Micro 5.1 x86_64
SLE Micro 5.1 arm64	SUSE Linux Enterprise Micro 5.1 aarch64
SLE Micro 5.1 s390x	SUSE Linux Enterprise Micro 5.1 s390x

过程：添加软件通道

- 在 Uyuni Web UI 中，导航到管理 > 安装向导 > 产品。
- 使用搜索栏找到适用于您的客户端操作系统和体系结构的产品，然后选中相应产品。这样会自动选中所有必需的通道。此外，建议的所有通道也将选中，并且 开关会打开。单击箭头以查看相关产品的完整列表，确保您需要的所有额外产品都已选中。
- 单击 并等待产品完成同步。

或者，您也可以在命令提示符处添加通道。此过程所需的通道包括：

表格 23. SLE Micro 产品 - CLI

OS Version	Base Channel	Updates Channel
SLE Micro 5.5 x86-64	sle-micro-5.5-pool-x86_64	sle-micro-5.5-updates-x86_64

OS Version	Base Channel	Updates Channel
SLE Micro 5.5 arm64	sle-micro-5.5-pool-arm64	sle-micro-5.5-updates-arm64
SLE Micro 5.5 IBM Z (s390x)	sle-micro-5.5-pool-s390x	sle-micro-5.5-updates-s390x
SLE Micro 5.4 x86_64	sle-micro-5.4-pool-x86_64	sle-micro-5.4-updates-x86_64
SLE Micro 5.4 arm64	sle-micro-5.4-pool-arm64	sle-micro-5.4-updates-arm64
SLE Micro 5.4 IBM Z (s390x)	sle-micro-5.4-pool-s390x	sle-micro-5.4-updates-s390x
SLE Micro 5.3 x86_64	sle-micro-5.3-pool-x86_64	sle-micro-5.3-updates-x86_64
SLE Micro 5.3 arm64	sle-micro-5.3-pool-arm64	sle-micro-5.3-updates-arm64
SLE Micro 5.3 IBM Z (s390x)	sle-micro-5.3-pool-s390x	sle-micro-5.3-updates-s390x
SLE Micro 5.2 x86_64	suse-microos-5.2-pool-x86_64	suse-microos-5.2-updates-x86_64
SLE Micro 5.2 arm64	suse-microos-5.2-pool-aarch64	suse-microos-5.2-updates-aarch64
SLE Micro 5.2 IBM Z (s390x)	suse-microos-5.2-pool-s390x	suse-microos-5.2-updates-s390x
SLE Micro 5.1 x86_64	suse-microos-5.1-pool-x86_64	suse-microos-5.1-updates-x86_64
SLE Micro 5.1 arm64	suse-microos-5.1-pool-aarch64	suse-microos-5.1-updates-aarch64
SLE Micro 5.1 IBM Z (s390x)	suse-microos-5.1-pool-s390x	suse-microos-5.1-updates-s390x

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `mgr-sync` 命令添加相应的通道：

```
mgr-sync add channel <channel_label_1>
mgr-sync add channel <channel_label_2>
mgr-sync add channel <channel_label_n>
```

2. 同步会自动启动。如果您要手动同步通道，请使用以下命令：

```
mgr-sync sync --with-children <channel_name>
```

3. 确保同步已完成，然后再继续操作。

要添加客户端工具，请在命令提示符处添加以下通道：

表格 24. SLE Micro 通道 - CLI

OS Version	Client Channel
SLE Micro 5.4	sle-micro-5.4-uyuni-client

OS Version	Client Channel
SLE Micro 5.3	suse-micro-5.3-uyuni-client
SLE Micro 5.2	suse-microos-5.2-uyuni-client
SLE Micro 5.1	sle-microos-5.1-uyuni-client

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。

4.2.2.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到**同步**选项卡，然后单击**同步**并选中**开始同步**。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `tail` 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.2.2.3. 注册客户端



SLE Micro clients require a reboot after registering.

Following the bootstrapping process, automatic booting is disabled on SLE Micro clients. This change was implemented due to intermittent automatic reboots, which could occur before Salt could relay the results of applying the bootstrap Salt state.

Although a reboot is automatically scheduled after registration is completed, it is respecting the default reboot manager maintenance window. This window may be several hours after the client is registered. It is advisable to manually reboot the client after the registration script finishes, to speed up the registration and to see the system appear in the system list.

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

对 SLE Micro 系统使用引导脚本时，请确保脚本的 certificate 部分包含以下内容：

```
ORG_CA_CERT=RHN-ORG-TRUSTED-SSL-CERT
ORG_CA_CERT_IS_RPM_YN=0
```

直接编辑引导脚本并添加该设置，或使用以下参数创建引导脚本：

```
mgr-bootstrap --script=bootstrap-sle-micro.sh \
--ssl-cert=/srv/www/htdocs/pub/RHN-ORG-TRUSTED-SSL-CERT
```

4.2.2.4. 重引导 SLE Micro

SLE Micro 是一种事务系统。事务更新一般支持数种重引导方法。建议在 Uyuni 所管理的系统中使用 `systemd` 来进行重引导。使用其他方法可能会导致系统出现意外行为。

如果 Uyuni 上的事务系统使用的是默认配置，引导该系统时，`systemd` 将会配置为引导方法 (`REBOOT_METHOD`)。该默认配置允许 Uyuni 控制重引导操作，重引导可以立即执行或使用 Uyuni 根据需要安排重引导时间。

4.2.2.4.1. 背景信息

默认情况下，在安装客户端的过程中会将重引导方法设置为 `auto`。采用 `auto` 引导方法时，如果 `rebootmgrd` 正在运行，将使用该服务根据配置的策略来重引导系统。策略可能设置为立即重引导或在维护时段重引导。有关详细信息，请参见 `rebootmgrd(8)` 手册页。如果 `rebootmgrd` 没有运行，Uyuni 将会调用

`systemctl reboot。`



使用 `systemd` 之外的任何其他方法都可能会导致系统出现意外行为。

4.2.3. 注册 SL Micro 客户端

本节包含有关注册运行 SL Micro 操作系统 6.0 x86-64、arm64 和 IBM Z (s390x) 的客户端的信息。

SL Micro 是一个超级可靠的轻量级操作系统，专为边缘计算而构建。它利用了 SUSE Linux Enterprise 的企业强化安全性和合规组件，并将它们整合到一个对开发人员友好的现代化、不可变操作系统平台。

SL Micro 使用事务更新。事务更新是原子更新（仅当所有更新都成功时，才应用所有更新）且支持回滚。它们不会影响正在运行的系统，因为在系统重引导之前，任何更改都不会生效。此信息显示在 **系统** > **细节** > **概览** 子选项卡中。

有关事务更新和重引导的详细信息，请访问 <https://documentation.suse.com/sles/html/SLES-all/cha-transactional-updates.html>。

4.2.3.1. 添加软件通道

将 SL Micro 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的产品包括：

表格 25. SL Micro 产品 - WebUI

操作系统版本	产品名称
SL Micro 6.0 x86-64	SUSE Linux Micro 6.0 x86_64
SL Micro 6.0 arm64	SUSE Linux Micro 6.0 arch64
SL Micro 6.0 s390x	SUSE Linux Micro 6.0 s390x

过程：添加软件通道

1. 在 Uyuni Web UI 中，导航到 **管理** > **安装向导** > **产品**。
2. 使用搜索栏找到适用于您的客户端操作系统和体系结构的产品，然后选中相应产品。这样会自动选中所有必需的通道。此外，建议的所有通道也将选中，并且 开关会打开。单击箭头以查看相关产品的完整列表，确保您需要的所有额外产品都已选中。
3. 单击 **[添加产品]** 并等待产品完成同步。

或者，您也可以在命令提示符处添加通道。此过程所需的通道包括：

表格 26. SL Micro 产品 - CLI

操作系统版本	基础通道
SL Micro 6.0 x86-64	sl-micro-6.0-pool-x86_64

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `mgr-sync` 命令添加相应的通道：

```
mgr-sync add channel <channel_label_1>
mgr-sync add channel <channel_label_2>
mgr-sync add channel <channel_label_n>
```

2. 同步会自动启动。如果您要手动同步通道，请使用以下命令：

```
mgr-sync sync --with-children <channel_name>
```

3. 确保同步已完成，然后再继续操作。

4.2.3.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到 **同步** 选项卡，然后单击 **同步** 并选中 **显示所有**。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `tail` 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.2.3.3. 注册客户端



SL Micro 客户端在注册后需要进行重引导。尽管系统在完成注册后会自动安排重引导，但会采用默认的重引导管理器维护时段。此时段在客户端注册后可能会持续几个小时。建议在注册脚本完成后手动重引导客户端，以加速注册过程并使系统显示在系统列表中。

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

对 SL Micro 系统使用引导脚本时，请确保脚本的 certificate 部分包含以下内容：

```
ORG_CA_CERT=RHN-ORG-TRUSTED-SSL-CERT
ORG_CA_CERT_IS_RPM_YN=0
```

直接编辑引导脚本并添加该设置，或使用以下参数创建引导脚本：

```
mgr-bootstrap --script=bootstrap-sl-micro.sh \
--ssl-cert=/srv/www/htdocs/pub/RHN-ORG-TRUSTED-SSL-CERT
```

4.2.3.4. 重引导 SL Micro

SL Micro 是一种事务系统。事务更新一般支持数种重引导方法。建议在 Uyuni 所管理的系统中使用 `systemd` 来进行重引导。使用其他方法可能会导致系统出现意外行为。

如果 Uyuni 上的事务系统使用的是默认配置，引导该系统时，`systemd` 将会配置为引导方法 (`REBOOT_METHOD`)。该默认配置允许 Uyuni 控制重引导操作，重引导可以立即执行或使用 Uyuni 根据需要安排重引导时间。

4.2.3.4.1. 背景信息

默认情况下，在安装客户端的过程中会将重引导方法设置为 `auto`。采用 `auto` 引导方法时，如果 `rebootmgrd` 正在运行，将使用该服务根据配置的策略来重引导系统。策略可能设置为立即重引导或在维护时段重引导。有关详细信息，请参见 `rebootmgrd(8)` 手册页。如果 `rebootmgrd` 没有运行，Uyuni 将会调用 `systemctl reboot`。



使用 `systemd` 之外的任何其他方法都可能会导致系统出现意外行为。

4.3. openSUSE 客户端注册

You can register openSUSE and openSUSE Leap Micro clients to your Uyuni Server. The method and details varies depending on the operating system of the client.

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。



Do not register a Uyuni Server to itself. The Uyuni Server must be managed individually or by using another separate Uyuni Server. For more information about using multiple servers, see [Specialized-guides > Large-deployments](#).

4.3.1. 注册 openSUSE Leap 客户端

This section contains information about registering clients running openSUSE operating systems. Uyuni supports openSUSE Leap 15 clients using Salt.

支持使用引导功能启动 openSUSE 客户端并执行初始状态运行，例如设置储存库和执行配置文件更新。

4.3.1.1. 添加软件通道

将 openSUSE 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

当前支持的系统结构为 `x86_64` 和 `aarch64`。有关支持的产品和体系结构的完整列表，请参见 [Client-configuration > Supported-features](#)。



下面的小节中的说明通常默认使用 `x86_64` 体系结构。请根据情况将其替换为其他体系结构。

例如，使用 `x86_64` 体系结构时，您需要如下产品：

表格 27. openSUSE 通道 - CLI

OS Version	openSUSE Leap 15.6	openSUSE Leap 15.5	openSUSE Leap 15.4
Base Channel	<code>opensuse_leap15_6</code>	<code>opensuse_leap15_5</code>	<code>opensuse_leap15_4</code>
Client Channel	<code>opensuse_leap15_6-uyuni-client</code>	<code>opensuse_leap15_5-uyuni-client</code>	<code>opensuse_leap15_4-uyuni-client</code>
Updates Channel	<code>opensuse_leap15_6-updates</code>	<code>opensuse_leap15_5-updates</code>	<code>opensuse_leap15_4-updates</code>
Non-OSS Channel	<code>opensuse_leap15_6-non-oss</code>	<code>opensuse_leap15_5-non-oss</code>	<code>opensuse_leap15_4-non-oss</code>
Non-OSS Updates Channel	<code>opensuse_leap15_6-non-oss-updates</code>	<code>opensuse_leap15_5-non-oss-updates</code>	<code>opensuse_leap15_4-non-oss-updates</code>
Backports Updates Channel	<code>opensuse_leap15_6-backports-updates</code>	<code>opensuse_leap15_5-backports-updates</code>	<code>opensuse_leap15_4-backports-updates</code>
SLE Updates Channel	<code>opensuse_leap15_6-sle-updates</code>	<code>opensuse_leap15_5-sle-updates</code>	<code>opensuse_leap15_4-sle-updates</code>

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

- 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

- 确保同步已完成，然后再继续操作。

4.3.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

- 在 Uyuni 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**同步**选项卡，然后单击**同步**并选中**开始同步**。

过程：在命令提示符处检查同步进度

- 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

- 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



openSUSE 通道可能会非常大。同步所需的时间可能会长达数小时。

4.3.1.3. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 **Client-configuration > Gpg-keys**。

4.3.1.4. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成

该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.3.2. Registering openSUSE Leap Micro Clients

This section contains information about registering clients running openSUSE Leap Micro operating systems on x86-64 and aarch64 architectures.

The openSUSE Leap Micro is an ultra-reliable, lightweight operating system purpose built for edge computing. It leverages the enterprise hardened security and compliance components of SUSE Linux Enterprise and merges them with a modern, immutable, developer-friendly OS platform.

The openSUSE Leap Micro uses transactional updates. Transactional updates are atomic (all updates are applied only if all updates succeed) and support rollbacks. They do not affect the running system because no changes are activated until the system is rebooted. This information is displayed in the [Systems > Details > Overview](#) subtab.

有关事务更新和重引导的详细信息，请访问 <https://documentation.suse.com/sles/html/SLES-all/cha-transactional-updates.html>。

表格 28. openSUSE 通道 - CLI

OS Version	openSUSE Leap Micro 5.5	openSUSE Leap Micro 5.4	openSUSE Leap Micro 5.3
Base Channel	opensuse_micro5_5	opensuse_micro5_4	opensuse_micro5_3
Client Channel	opensuse_micro5_5-uyuni-client	opensuse_micro5_4-uyuni-client	opensuse_micro5_3-uyuni-client
SLE Updates Channel	opensuse_micro5_5-sle-updates	opensuse_micro5_4-sle-updates	opensuse_micro5_3-sle-updates

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 spacewalk-common-channels 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。

4.3.2.1. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到同步选项卡，然后单击同步并选中同步复选框。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



openSUSE Leap Micro channels can be very large. Synchronization can sometimes take several hours.

4.3.2.2. 注册客户端



openSUSE Leap Micro clients require reboot after registering.

Following the bootstrapping process, automatic booting is disabled on openSUSE Leap Micro. This change was implemented due to intermittent automatic reboots, which could occur before Salt could relay the results of applying the bootstrap salt state.

Reboot is automatically scheduled after registration is completed, but it is respecting the default reboot manager maintenance window. This window may be several hours after the client is registered. To speed up openSUSE Leap Micro registration, manually reboot the client after the registration script finishes.

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.4. Alibaba Cloud Linux 客户端注册

您可以将 Alibaba Cloud Linux 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.4.1. 注册 Alibaba Cloud Linux 客户端

This section contains information about registering clients running Alibaba Cloud Linux operating systems.



一些 Alibaba Cloud Linux 2 实例需要尝试两次才能成功注册。

4.4.1.1. 添加软件通道

将 Alibaba Cloud Linux 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 29. Alibaba Cloud Linux 通道 - CLI

操作系统版本	核心通道	更新通道	客户端通道
Alibaba Cloud Linux 2	alibaba-2	alibaba-2-updates	alibaba-2-uyuni-client

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 spacewalk-common-channels 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。

4.4.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到同步选项卡，然后单击同步并选中同步。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.4.1.3. 创建激活密钥

您需要创建与您的 Alibaba Cloud Linux 通道关联的激活密钥。

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.4.1.4. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

Some Alibaba Cloud Linux 2 instances will fail to register on the first try. This is due to a known bug in the Alibaba Cloud Linux 2 image.

`python-urlgrabber3` 软件包以 Python pip 软件包和 RPM 软件包两种形式提供，这可能会导致在首次尝试注册时发生冲突。

如果您的实例基于其中一个受影响的映像版本，客户端在第二次尝试注册时应该会正确注册。

4.5. AlmaLinux 客户端注册

您可以将 AlmaLinux 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您必须已创建激活密钥。

- 有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。
- 有关将 AlmaLinux 迁移到 SUSE Liberty Linux 的详细信息，请参见 [client-configuration:clients-sleses.pdf](#)。

4.5.1. 注册 AlmaLinux 客户端

This section contains information about registering clients running AlmaLinux operating systems.



如果 AlmaLinux 实例是在 AWS 中创建的，则 `/etc/machine-id` 中的 `machine-id` ID 一律相同。请务必在创建实例后重新生成 `machine-id`。有关详细信息，请参见 [Administration > Troubleshooting](#)。

4.5.1.1. 添加软件通道



我们已使用 `--enforcing` 策略并采用默认的 SELinux 配置对将 AlmaLinux 客户端注册到 Uyuni 的过程进行了测试。将 AlmaLinux 客户端注册到 Uyuni 时，您无需禁用 SELinux。

将 AlmaLinux 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

目前支持的系统结构有 `x86_64` 和 `aarch64`，在版本 9 上，另外还支持 `ppc64le` 和 `s390x`。有关支持的产品和体系结构的完整列表，请参见 [Client-configuration > Supported-features](#)。



下面的小节中的说明通常默认使用 `x86_64` 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 30. AlmaLinux 通道 - CLI

操作系统版本	基础通道	客户端通道	AppStream 通道
AlmaLinux 9	<code>almalinux9</code>	<code>almalinux9-uyuni-client</code>	<code>almalinux9-appstream</code>
AlmaLinux 8	<code>almalinux8</code>	<code>almalinux8-uyuni-client</code>	<code>almalinux8-appstream</code>

过程：在命令提示符处添加软件通道

- 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道。请确保指定正确的体系结构：

```
spacewalk-common-channels \
-a <体系结构> \
<基础通道名称> \
<子通道名称 1> \
<子通道名称 2> \
... <子通道名称 n>
```

- 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <base_channel_label>-<architecture>
```

- 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。



对于 AlmaLinux 9 和 AlmaLinux 8 客户端，请添加基础通道和 AppStream 通道。您需要来自这两个通道的软件包。如果未添加这两个通道，将会因缺少软件包而无法创建引导储存库。

如果您使用的是模块化通道，则必须在 AlmaLinux 8 客户端上启用 Python 3.6 模块流。如果不提供 Python 3.6，spacecmd 软件包安装将会失败。



您可能会发现 AppStream 通道中提供的软件包数量在上游通道和 Uyuni 通道之间存在一定的差异。如果您对在不同时间添加的同一通道进行比较，会发现其数量也不相同。这是由 AlmaLinux 管理其储存库的方式所致。当有新版本发布时，AlmaLinux 会去除软件包的较旧版本，而 Uyuni 则会保留所有版本，无论新旧与否。

4.5.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

- 在 Uyuni 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 **同步** 选项卡，然后单击 **同步** 并选中 **开始同步**。

过程：在命令提示符处检查同步进度

- 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

- 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.5.1.3. 创建激活密钥

您需要创建与您的 AlmaLinux 通道关联的激活密钥。

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.5.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



Trusting a GPG key is important for security on clients. It is the task of the administrator to decide which keys are needed and can be trusted. Because a software channel cannot be used when the GPG key is not trusted, the decision of assigning a channel to a client depends on the decision of trusting the key.

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。

4.5.1.5. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.5.1.6. 管理勘误

当您更新 AlmaLinux 客户端时，软件包会包含有关更新的元数据。

4.6. Amazon Linux 客户端注册

您可以将 Amazon Linux 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.6.1. 注册 Amazon Linux 客户端

This section contains information about registering clients running Amazon Linux operating systems.



When created at AWS, Amazon Linux 2 instances always have the same machine-id id at /etc/machine-id. If you are creating Amazon Linux 2 instances, make sure you regenerate the machine-id after the instances are created. For more information, see [Administration > Troubleshooting](#).

Amazon Linux 2023 is not affected by this.

4.6.1.1. 添加软件通道

将 Amazon Linux 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

当前支持的系统结构为 x86_64 和 aarch64。有关支持的产品和体系结构的完整列表，请参见 [Client-configuration > Supported-features](#)。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 31. Amazon Linux Channels - CLI

OS Version	Base Channel	Client Channel
Amazon Linux 2023	amazonlinux2023	amazonlinux2023-uyuni-client
Amazon Linux 2	amazonlinux2-core	amazonlinux2-uyuni-client



For Amazon Linux 2, make sure you also add and synchronize amazonlinux2-extra-docker channel if you plan to use Docker at your Amazon Linux instances.



For Amazon Linux 2023, make sure you also add and synchronize amazonlinux2023-kernel-livepatch channel if you plan to use Kernel Live patches at your Amazon Linux instances.

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 spacewalk-common-channels 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

- 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

- 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。

4.6.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

- 在 Uyuni 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**同步**选项卡，然后单击**同步**并选中**开始同步**。

过程：在命令提示符处检查同步进度

- 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

- 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.6.1.3. 创建激活密钥

您需要创建与您的 Amazon Linux 通道关联的激活密钥。

有关激活密钥的详细信息，请参见 **Client-configuration** > **Activation-keys**。

4.6.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 **Client-configuration** > **Gpg-keys**。

4.6.1.5. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.7. CentOS 客户端注册

您可以将 CentOS 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您必须已创建激活密钥。

- 有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。
- 有关将 CentOS 迁移到 SUSE Liberty Linux 的详细信息，请参见 [client-configuration:clients-sleses.pdf](#)。

4.7.1. 注册 CentOS 客户端

This section contains information about registering clients running CentOS operating systems.



You are responsible for arranging access to CentOS base media repositories and CentOS installation media, as well as connecting Uyuni Server to the CentOS content delivery network.



我们已使用 `--enforcing` 策略并采用默认的 SELinux 配置对将 CentOS 客户端注册到 Uyuni 的过程进行了测试。将 CentOS 客户端注册到 Uyuni 时，您无需禁用 SELinux。

4.7.1.1. 添加软件通道

将 CentOS 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

当前支持的系统结构为 `x86_64` 和 `aarch64`。有关支持的产品和体系结构的完整列表，请参见 [Client-configuration > Supported-features](#)。



下面的小节中的说明通常默认使用 `x86_64` 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 32. CentOS 通道 - CLI

操作系统版本	基础通道	客户端通道	更新/Appstream 通道
CentOS 7	centos7	centos7-uyuni-client	centos7-updates

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道。请确保指定正确的体系结构：

```
spacewalk-common-channels \
-a <体系结构> \
<基础通道名称> \
<子通道名称 1> \
<子通道名称 2> \
... <子通道名称 n>
```

2. 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <base_channel_label>-<architecture>
```

3. 确保同步已完成，然后再继续操作。



`spacewalk-common-channels` 提供的客户端工具通道来自 Uyuni 而非 SUSE。

如果您使用的是模块化通道，则必须在客户端上启用 Python 3.6 模块流。如果不提供 Python 3.6，`spacecmd` 软件包安装将会失败。



您可能会发现 AppStream 通道中提供的软件包数量在上游通道和 Uyuni 通道之间存在一定的差异。如果您对在不同时间添加的同一通道进行比较，会发现其数量也不相同。这是由 CentOS 管理其储存库的方式所致。当有新版本发布时，CentOS 会去除软件包的较旧版本，而 Uyuni 则会保留所有版本，无论新旧与否。

4.7.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到 **同步** 选项卡，然后单击 **同步** 并选中 **开始同步**。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `tail` 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.7.1.3. 创建激活密钥

您需要创建与您的 CentOS 通道关联的激活密钥。

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.7.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。

4.7.1.5. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.7.1.6. 管理勘误



This section is only applicable to non-containerized Uyuni and it will be removed after CentOS 7 will go end-of-life.

当您更新 CentOS 客户端时，软件包不包含有关更新的元数据。您可以使用第三方勘误服务来获取此信息。



CEFS 的作者会按照尽力而为的原则提供补丁或勘误，希望它们有用，但无法保证其正确性或及时性。这意味着补丁日期可能不正确，且至少在一种情况下所显示的发布数据滞后一个多月。有关这些情况的详细信息，请参见 <https://github.com/stevemeier/cefs/issues/28#issuecomment-656579382> 和 <https://github.com/stevemeier/cefs/issues/28#issuecomment-656573607>。

任何有关补丁数据的问题或滞后都可能导致将不可靠的补丁信息导入到您的 Uyuni 服务器中，进而导致报告、审计、CVE 更新或其他与补丁相关的信息也不正确。请考虑使用其他方案来替代此服务，例如独立校验补丁数据或选择其他操作系统，具体取决于您的安全相关要求和认证准则。

过程：安装勘误服务

1. On the Uyuni Server, from the command prompt, as root, add the `sle-module-development-tools` module:

```
SUSEConnect --product sle-module-development-tools/15.2/x86_64
```

2. 安装勘误服务依赖项：

```
zypper in perl-Text-Unidecode
```

3. 在 `/etc/rhn/rhn.conf` 中添加或编辑下面一行：

```
java.allow_adding_patches_via_api = centos7-x86_64-updates,centos7-x86_64,centos7-x86_64-extras
```

4. 重启 Tomcat：

```
systemctl restart tomcat
```

5. 为勘误脚本创建一个文件：

```
touch /usr/local/bin/cent-errata.sh
```

6. 编辑新文件以包含此脚本，并视需要编辑储存库细节。此脚本会从外部勘误服务提取勘误细节，将其解压缩，然后发布这些细节：

```
#!/bin/bash
mkdir -p /usr/local/centos
cd /usr/local/centos
rm *.xml
wget -c http://cefs.steve-meier.de/errata.latest.xml
wget -c https://www.redhat.com/security/data/oval/v2/RHEL7/rhel-
7.oval.xml.bz2
bzip2 -d rhel-7.oval.xml.bz2
wget -c http://cefs.steve-meier.de/errata-import.tar
tar xvf errata-import.tar
chmod +x /usr/local/centos/errata-import.pl
export SPACEWALK_USER='<adminname>' ; export
SPACEWALK_PASS='<password>'
/usr/local/centos/errata-import.pl --server '<servername>' \
--errata /usr/local/centos/errata.latest.xml \
--include-channels=centos7-x86_64-updates,centos7-x86_64,centos7-
-x86_64-extras \
--publish --rhsa-oval /usr/local/centos/rhel-7.oval.xml
```

7. 设置 cron 作业以每日运行该脚本：

```
ln -s /usr/local/bin/cent-errata.sh /etc/cron.daily
```

有关此工具的详细信息，请参见 <https://cefs.steve-meier.de/>。

4.8. Debian 客户端注册

您可以将 Debian 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.8.1. 注册 Debian 客户端

This section contains information about registering clients running Debian operating systems.

可以通过引导 Debian 客户端来执行初始状态的运行以及配置文件的更新。

4.8.1.1. 准备注册

您需要完成一些准备工作，然后才能将 Debian 客户端注册到 Uyuni 服务器：

- 确保 DNS 配置正确并提供客户端对应的项。或者，您也可以配置 Uyuni 服务器和客户端上的 /etc/hosts 文件，在其中添加相应的项。
- 注册前，客户端的日期和时间必须已与 Uyuni 服务器同步。

4.8.1.2. 添加软件通道

将 Debian 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 33. Debian 通道 - CLI

OS Version	Base Channel	Client Channel	Updates Channel	Security Channel
Debian 12	debian-12-pool-amd64-uyuni	debian-12-amd64-uyuni-client	debian-12-amd64-main-updates-uyuni	debian-12-amd64-main-security-uyuni
Debian 11	debian-11-pool-amd64-uyuni	debian-11-amd64-uyuni-client	debian-11-amd64-main-updates-uyuni	debian-11-amd64-main-security-uyuni

过程：在命令提示符处添加软件通道

- 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 spacewalk-common-channels 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

- 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

- 确保同步已完成，然后再继续操作。

4.8.1.3. 检查同步状态

过程：在 Web UI 中检查同步进度

- 在 Uyuni 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。

2. 导航到“同步”选项卡，然后单击“开始”并选中“Debian”。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



Debian 通道可能会非常大。同步所需的时间可能会长达数小时。

4.8.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。



Debian 客户端可能需要安装多个 GPG 密钥。

同步第三方 Debian 储存库时，您需要在服务器上导入相应的 GPG 密钥。如果缺少 GPG 密钥，同步将会失败。

使用 Debian 储存库时，系统只会对元数据签名。因此不需要导入软件通道的 GPG 密钥。Uyuni 将不会对软件包重新签名。

要查看已导入 Uyuni 服务器的 GPG 密钥，请运行以下命令：

```
mgrctl exec -- gpg --homedir /var/lib/spacewalk/gpgdir --list-keys
```

To import a new GPG key, run the following command:

```
mgradm gpg add <filename>.gpg
```

4.8.1.5. Root 访问权限

默认会为 Debian 上的 root 用户禁用 SSH 访问权限。

要想能够使用普通用户进行初始配置，您需要编辑 `sudoers` 文件。

过程：向 Root 用户授予访问权限

1. 在客户端上，编辑 `sudoers` 文件：

```
sudo visudo
```

在 `sudoers` 文件末尾添加下面一行，以向用户授予 `sudo` 访问权限。以在 Web UI 中引导客户端的用户的名称替换 `<user>`：

```
<user>  ALL=NOPASSWD: /usr/bin/python, /usr/bin/python2,  
/usr/bin/python3, /var/tmp/venv-salt-minion/bin/python
```



此过程无需口令便可授予 `root` 访问权限，而注册客户端需要提供口令。客户端成功安装后会以 `root` 特权运行，因此将不再需要该访问权限。客户端成功安装之后，建议您从 `sudoers` 文件中去除该行。

4.8.1.6. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.9. OpenEuler Client Registration

You can register openEuler clients to your Uyuni Server. The method and details varies depending on the operating system of the client.

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.9.1. Registering openEuler Clients

This section contains information about registering clients running openEuler operating systems.



When created at AWS, openEuler instances always have the same machine-id id at /etc/machine-id. Make sure you regenerate the machine-id after the instance is created. For more information, see **Administration > Troubleshooting**.

4.9.1.1. 添加软件通道

Before you register openEuler clients to your Uyuni Server, you need to add the required software channels, and synchronize them.

当前支持的系统结构为 x86_64 和 aarch64。有关支持的产品和体系结构的完整列表，请参见 **Client-configuration > Supported-features**。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 34. openEuler Channels - CLI

OS Version	Core Channel	Client Channel	Update Channel	EPOL Channel	Everything Channel
openEuler 22.03	openeuler2203	openeuler2203-uyuni-client	openeuler2203-update	openeuler2203-epol	openeuler2203-everything

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 spacewalk-common-channels 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。

4.9.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到——选项卡，然后单击——并选中——。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.9.1.3. 创建激活密钥

You need to create an activation key that is associated with your openEuler channels.

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.9.1.4. 在客户端上信任 GPG 密钥

4.9.1.5. 在客户端上信任 GPG 密钥

操作系统要么直接信任自己的 GPG 密钥，要么至少将它们与最小系统一起安装，但通过其他 GPG 密钥签名的第三方软件包需要手动处理。客户端可以在不信任 GPG 密钥的情况下成功引导，但除非密钥受信任，否则您将无法安装新的客户端工具软件包或更新软件包。

Clients now use GPG key information entered for a software channel to manage the trusted keys. When a software channel with GPG key information is assigned to a client, the key is trusted when the channel is refreshed or the first package is installed from this channel.

软件通道页面中的 GPG 密钥 URL 参数可以包含以空格分隔的多个密钥 URL。如果其为文件 URL，则必须在使用软件通道之前在客户端上部署 GPG 密钥文件。

The GPG keys for the Client Tools Channels of Red Hat based clients are deployed on the client into /etc/pki/rpm-gpg/ and can be referenced with file URLs.

Only in case a software channel is assigned to the client they will be imported and trusted by the system.



由于基于 Debian 的系统仅会对元数据签名，因此不需要为各个通道指定确切的密钥。如果用户按 [Administration > Repo-metadata](#) 中的“使用自己的 GPG 密钥”所述配置了自己的 GPG 密钥来对元数据签名，系统会自动部署并信任该密钥。

4.9.1.5.1. 用户定义的 GPG 密钥

Users can define custom GPG keys to be deployed to a client.

通过提供某些 pillar 数据并在 Salt 文件系统中提供 GPG 密钥文件，系统会自动将它们部署到客户端。

这些密钥会分别部署到 `/etc/pki/rpm-gpg/`（在基于 RPM 的操作系统上）和 `/usr/share/keyrings/`（在 Debian 系统上）中：

为您的要将密钥部署到的客户端定义 pillar 键 `custom_gpgkeys` 并列出密钥文件名。

```
cat /srv/pillar/mypillar.sls
custom_gpgkeys:
  - my_first_gpg.key
  - my_second_gpgkey.gpg
```

此外，在 Salt 文件系统中创建名为 `gpg` 的目录，并将 `custom_gpgkeys` pillar 数据中所指定的 GPG 密钥文件存储在该目录下。

```
ls -la /srv/salt/gpg/
/srv/salt/gpg/my_first_gpg.key
/srv/salt/gpg/my_second_gpgkey.gpg
```

The keys are deployed to the client at `/etc/pki/rpm-gpg/my_first_gpg.key` and `/etc/pki/rpm-gpg/my_second_gpgkey.gpg`.

最后一步是将 URL 添加到软件通道的“GPG 密钥 URL”字段中。请导航到 **软件** > **管理** > **通道**，然后选择要修改的通道。将值 `file:///etc/pki/rpm-gpg/my_first_gpg.key` 添加到 GPG 公钥 URL 中。

4.9.1.5.2. 引导脚本中的 GPG 密钥

过程：在客户端上使用引导脚本信任 GPG 密钥

1. 在 Uyuni 服务器上的命令提示符处，检查 `/srv/www/htdocs/pub/` 目录的内容。此目录包含所有可用的公共密钥。记下为您正在注册的客户端指派的通道适用的密钥。
2. 打开相关的引导脚本，找到 `ORG_GPG_KEY=` 参数并添加所需的密钥。例如：

```
uyuni-gpg-pubkey-0d20833e.key
```

您无需删除任何以前存储的密钥。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。如果不信任 GPG 密钥，便无法为客户端指派软件通道。

4.9.1.6. 注册客户端

openEuler clients are registered in the same way as all other clients. For more information, see **Client-configuration > Registration-overview**.

4.10. Oracle 客户端注册

您可以将 Oracle Linux 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您必须已创建激活密钥。

- 有关创建激活密钥的详细信息，请参见 **Client-configuration > Activation-keys**。
- 有关将 Oracle Linux 迁移到 SUSE Liberty Linux 的详细信息，请参见 [client-configuration:clients-sleses.pdf](#)。

4.10.1. 注册 Oracle Linux 客户端

This section contains information about registering clients running Oracle Linux operating systems.



目前不支持直接将 Unbreakable Linux Network (ULN) 储存库与 Uyuni 同步。必须使用 ULN 的 Oracle 本地发行版。有关设置本地 ULN 镜像的详细信息，请参见 <https://docs.oracle.com/en/operating-systems/oracle-linux/software-management/sfw-mgmt-UseSoftwareDistributionMirrors.html#local-uln-mirror> 上提供的相关 Oracle 文档。

4.10.1.1. 添加软件通道

将 Oracle Linux 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

当前支持的系统结构为 `x86_64` 和 `aarch64`。有关支持的产品和体系结构的完整列表，请参见 **Client-configuration > Supported-features**。



下面的小节中的说明通常默认使用 `x86_64` 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 35. Oracle 通道 - CLI

操作系统版本	基础通道	客户端通道	更新通道
Oracle Linux 9	oraclelinux9	oraclelinux9-uyuni-client	oraclelinux9-appstream
Oracle Linux 8	oraclelinux8	oraclelinux8-uyuni-client	oraclelinux8-appstream

操作系统版本	基础通道	客户端通道	更新通道
Oracle Linux 7	oraclelinux7	oraclelinux7-uyuni-client	-

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。



对于 Oracle Linux 9 和 Oracle Linux 8 客户端，请添加基础通道和 AppStream 通道。您需要来自这两个通道的软件包。如果未添加这两个通道，将会因缺少软件包而无法创建引导储存库。

如果您使用的是模块化通道，则必须在客户端上启用 Python 3.6 模块流。如果不提供 Python 3.6，`spacecmd` 软件包安装将会失败。

4.10.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到 **同步** 选项卡，然后单击 **同步** 并选中 **所有通道**。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `tail` 命令检查同步日志文件：

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

- 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.10.1.3. 创建激活密钥

您需要创建与您的 Oracle Linux 通道关联的激活密钥。

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.10.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。



对于 Oracle Linux 9 或 Oracle Linux 8 客户端，请使用

`ol8-gpg-pubkey-82562EA9AD986DA3.key`

对于 Oracle Linux 7 客户端，请使用

`ol67-gpg-pubkey-72F97B74EC551F0A3.key`

4.10.1.5. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.11. Raspberry Pi OS Client Registration

You can register Raspberry Pi OS clients to your Uyuni Server. The method and details depend on the operating system of the client.

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.11.1. Registering Raspberry Pi OS Clients

This section contains information about registering clients running Raspberry Pi OS operating systems.

Bootstrapping can be used with Raspberry Pi OS clients for performing initial state runs, and for profile updates.

4.11.1.1. 准备注册

Some preparation is required before you can register Raspberry Pi OS clients to the Uyuni Server:

- 确保 DNS 配置正确并提供客户端对应的项。或者，您也可以配置 Uyuni 服务器和客户端上的 `/etc/hosts` 文件，在其中添加相应的项。
- 注册前，客户端的日期和时间必须已与 Uyuni 服务器同步。

4.11.1.2. 添加软件通道

Before you register Raspberry Pi OS clients to your Uyuni Server, you need to add the required software channels, and synchronize them.

The architectures currently supported are: arm64 and armhf. For full list of supported products and architectures, see [Client-configuration > Supported-features](#).

此过程所需的通道包括：

表格 36. Raspberry Pi OS Channels - CLI

Channel description	arm64	armhf
Base Channel	raspberrypios-12-pool-arm64-uyuni	raspberrypios-12-pool-armhf-uyuni
Client Channel	raspberrypios-12-arm64-uyuni-client	raspberrypios-12-armhf-uyuni-client
Updates Channel	raspberrypios-12-arm64-main-updates-uyuni	-
Contributions Channel	raspberrypios-12-arm64-contrib-uyuni	raspberrypios-12-armhf-contrib-uyuni
Non Free Channel	raspberrypios-12-arm64-non-free-uyuni	raspberrypios-12-armhf-non-free-uyuni
Non Free Firmware Channel	raspberrypios-12-arm64-non-free-firmware-uyuni	-
Raspberry Channel	raspberrypios-12-arm64-raspberry-uyuni	raspberrypios-12-armhf-raspberry-uyuni

Channel description	arm64	armhf
Contribution Updates	raspberrypios-12-arm64-contrib-updates-uyuni	-
Non Free Updates	raspberrypios-12-arm64-non-free-updates-uyuni	-
Non Free Firmware Updates	raspberrypios-12-arm64-non-free-firmware-updates-uyuni	-
Security Main Channel	raspberrypios-12-arm64-main-security-uyuni	-
Security Contribution Channel	raspberrypios-12-arm64-contrib-security-uyuni	-
Security Non Free Channel	raspberrypios-12-arm64-non-free-security-uyuni	-
Security Non Free Firmware Channel	raspberrypios-12-arm64-non-free-firmware-security-uyuni	-
RPI Channel	-	raspberrypios-12-armhf-rpi-uyuni

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。



You need all the new channels fully synchronized before bootstrapping any Raspberry Pi OS client.

4.11.1.3. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到——选项卡，然后单击——并选中——。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



Raspberry Pi OS channels can be very large. Synchronization can sometimes take several hours.

4.11.1.4. 创建激活密钥

You need to create an activation key that is associated with your Raspberry Pi OS channels.

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.11.1.5. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。



Raspberry Pi OS clients can require multiple GPG keys to be installed.

When synchronizing third-party Raspberry Pi OS repositories, you will need to import the appropriate GPG key on the server. If the GPG key is missing, synchronization will fail.

For Raspberry Pi OS repositories, only the metadata is signed. Therefore importing a GPG key for the software channel is not needed. Packages will not be re-signed by Uyuni.

要查看已导入 Uyuni 服务器的 GPG 密钥，请运行以下命令：

```
mgrctl exec -- gpg --homedir /var/lib/spacewalk/gpgdir --list-keys
```

To import a new GPG key, run the following command:

```
mgradm gpg add <filename>.gpg
```

4.11.1.6. Root 访问权限

The root user on Raspberry Pi OS is disabled by default for SSH access.

要想能够使用普通用户进行初始配置，您需要编辑 `sudoers` 文件。

过程：向 Root 用户授予访问权限

1. 在客户端上，编辑 `sudoers` 文件：

```
sudo visudo
```

在 `sudoers` 文件末尾添加下面一行，以向用户授予 `sudo` 访问权限。以在 Web UI 中引导客户端的用户的名称替换 `<user>`：

```
<user> ALL=NOPASSWD: /usr/bin/python, /usr/bin/python2,
/usr/bin/python3, /var/tmp/venv-salt-minion/bin/python
```



此过程无需口令便可授予 `root` 访问权限，而注册客户端需要提供口令。客户端成功安装后会以 `root` 特权运行，因此将不再需要该访问权限。客户端成功安装之后，建议您从 `sudoers` 文件中去除该行。

4.11.1.7. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.12. Red Hat 客户端注册

您可以使用 Red Hat 内容分发网络 (CDN) 或 Red Hat 更新基础结构 (RHUI) 将 Red Hat Enterprise Linux 客户

端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您必须已创建激活密钥。

- 有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。
- 有关将 Red Hat Enterprise Linux 迁移到 SUSE Liberty Linux 的详细信息，请参见 [client-configuration:clients-sleses.pdf](#)。

4.12.1. 使用 CDN 注册 Red Hat Enterprise Linux 客户端

This section contains information about using the Red Hat content delivery network (CDN) to register clients running Red Hat Enterprise Linux operating systems.

而有关使用 Red Hat 更新基础结构 (RHUI) 的信息，请参见 [Client-configuration > Clients-rh-rhui](#)。



You are responsible for arranging access to Red Hat base media repositories and RHEL installation media, as well as connecting Uyuni Server to the Red Hat content delivery network. You must obtain support from Red Hat for all your RHEL systems. If you do not do this, you might be violating your terms with Red Hat.

4.12.1.1. 导入权利和证书

Red Hat 客户端需要 Red Hat 证书颁发机构 (CA) 和权利证书以及权利密钥。

权利证书内嵌失效日期，与支持订阅的期限匹配。为避免服务中断，您需要在每个支持订阅期结束时重复此过程。

Red Hat 提供了一个订阅管理器工具，可用于管理订阅指派。此工具在本地运行，可跟踪安装的产品和订阅。客户端必须在订阅管理器中注册才能获得证书。

Red Hat 客户端使用 URL 来复制储存库。URL 更改取决于 Red Hat 客户端是在何处注册的。

Red Hat 客户端可通过三种方式注册：

- redhat.com 上的 Red Hat 内容分发网络 (CDN)
- Red Hat 从属服务器
- 云中的 Red Hat 更新基础结构 (RHUI)

本指南将介绍注册到 Red Hat CDN 的客户端。您至少须有一个注册到 CDN 的系统并拥有授权订阅，以获得储存库内容。

而有关使用 Red Hat 更新基础结构 (RHUI) 的信息，请参见 [Client-configuration > Clients-rh-rhui](#)。



要为客户端系统使用从属证书，必须有从属服务器和订阅。Uyuni 服务器不支持使用从属证书的客户端。



权利证书内嵌失效日期，与支持订阅的期限匹配。为避免服务中断，您需要在每个支持订阅期结束时重复此过程。

Red Hat 提供了订阅管理器工具，可用于管理订阅指派。此工具在客户端系统本地运行，可跟踪安装的产品和订阅。使用订阅管理器注册到 redhat.com，然后执行下列过程获得证书。

过程：将客户端注册到订阅管理器

1. 在客户端系统上的命令提示符处注册订阅管理器工具：

```
subscription-manager register
```

出现提示时，输入您的 Red Hat 门户用户名和口令。

2. 运行命令：

```
subscription-manager activate
```

3. 将客户端系统中的权利证书和密钥复制到 Uyuni 服务器可访问的位置：

```
cp /etc/pki/entitlement/ <example>/entitlement/
```



您的权利证书和密钥的文件扩展名均为 .pem。密钥的文件名中还包含 key。

4. 将客户端系统中的 Red Hat CA 证书文件复制到权利证书和密钥所在的相同网络位置：

```
cp /etc/rhsm/ca/redhat-uep.pem <example>/entitlement
```

要管理 Red Hat 客户端上的储存库，您需要将 CA 和权利证书导入 Uyuni 服务器。这需要您执行三次导入过程以创建相应的三项：三项分别对应权利证书、权利密钥和 Red Hat 证书。

过程：将证书导入服务器

1. 在 Uyuni 服务器 Web UI 上，导航到 **系统**，**自动安装**，**GPG 和 SSL 密钥**。

2. 单击 **[创|建|存|储|的|密|钥/|证|书]**，并为权利证书设置下列参数：

- 在 **Entitlement-Cert-date** 字段中键入 Entitlement-Cert-date。
- 在 **SSL** 字段中，选择 SSL。

- 在“-----”字段中，浏览到您保存权利证书的位置，然后选择 .pem 证书文件。

3. 单击 **[创建密钥]**。

4. 单击 **[创建存储的密钥/证书]**，并为权利密钥设置下列参数：

- 在“-----”字段中键入 Entitlement-key-date。
- 在“-----”字段中，选择 SSL。
- 在“-----”字段中，浏览到您保存权利密钥的位置，然后选择 .pem 密钥文件。

5. 单击 **[创建密钥]**。

6. 单击 **[创建存储的密钥/证书]**，并为 Red Hat 证书设置下列参数：

- 在“-----”字段中键入 redhat-uep。
- 在“-----”字段中，选择 SSL。
- 在“-----”字段中，浏览到您保存 Red Hat 证书的位置，然后选择证书文件。

7. 单击 **[创建密钥]**。

4.12.1.2. 添加软件通道

将 Red Hat 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 37. Red Hat 通道 - CLI

OS Version	Base Channel	Client Channel	Tools Channel
Red Hat 9	rhel9-pool-uyuni	-	rhel9-uyuni-client
Red Hat 8	rhel8-pool-uyuni	-	rhel8-uyuni-client
Red Hat 7	rhel7-pool-uyuni	-	rhel7-uyuni-client

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 spacewalk-common-channels 命令添加相应的通道。请确保指定正确的体系结构：

```
spacewalk-common-channels \
-a <体系结构> \
<基础通道名称> \
<子通道名称 1> \
<子通道名称 2> \
... <子通道名称 n>
```

- 如果 **自动同步** 处于关闭状态, 请同步通道:

```
spacewalk-repo-sync -p <base_channel_label>-<architecture>
```

- 确保同步已完成, 然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。

4.12.1.3. 准备自定义储存库和通道

To mirror the software from the Red Hat CDN, you need to create custom channels and repositories in Uyuni that are linked to the CDN by a URL. You must have entitlements to these products in your Red Hat Portal for this to work correctly. You can use the subscription manager tool to get the URLs of the repositories you want to mirror:

```
subscription-manager repos
```

可以使用这些储存库 URL 来创建自定义储存库。这样您便可只镜像管理客户端所需的内容。



如果您在 Red Hat 门户中拥有正确的权利, 就可以只创建 Red Hat 储存库的自定义版本。

此过程所需的细节包括:

表格 38. Red Hat 自定义储存库设置

选项	设置
储存库 URL	Red Hat CDN 提供的内容 URL
包含已签名的元数据?	取消选中所有 Red Hat Enterprise 储存库
SSL CA 证书	redhat-uep
SSL 客户端证书	Entitlement-Cert-date
SSL 客户端密钥	Entitlement-Key-date

过程: 创建自定义储存库

- 在 Uyuni 服务器 Web UI 上, 导航到**软件** > **管理** > **储存库**。
- 单击 **[创建储存库]**, 然后为储存库设置适当的参数。
- 单击 **[创建储存库]**。
- 对需要创建的所有储存库重复以上步骤。

此过程所需的通道包括:

表格 39. Red Hat 自定义通道

OS Version	Base Channel
Red Hat 9	rhel9-pool-uyuni
Red Hat 8	rhel8-pool-uyuni
Red Hat 7	rhel7-pool-uyuni

过程：创建自定义通道

1. 在 Uyuni 服务器 Web UI 上，导航到软件，管理，通道。
2. 单击 ，然后为通道设置相应的参数。
3. 在-----字段中，选择相应的基础通道。
4. 单击 。
5. 对需要创建的所有通道重复以上步骤。每个自定义储存库都应该有一个自定义通道。

您可以导航到软件，通道列表，所有，以检查是否已创建所有相应的通道和储存库。



对于 Red Hat 8 客户端，请添加基础通道和 AppStream 通道。您需要来自这两个通道的软件包。如果未添加这两个通道，将会因缺少软件包而无法创建引导储存库。

如果您使用的是模块化通道，则必须在客户端上启用 Python 3.6 模块流。如果不提供 Python 3.6，spacecmd 软件包安装将会失败。

创建所有通道之后，可以将其与您创建的储存库关联：

过程：将通道与储存库关联

1. 在 Uyuni 服务器 Web UI 上，导航到软件，管理，通道，然后单击要关联的通道。
2. 导航到-----选项卡，然后选中要与此通道关联的储存库。
3. 单击  以将通道与储存库相关联。
4. 对需要关联的所有通道和储存库重复以上步骤。
5. 可选：导航到-----选项卡，为此储存库设置定期同步日程安排。
6. 单击  以立即开始同步。

4.12.1.4. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到-----选项卡，然后单击-----并选中-----。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



Red Hat Enterprise Linux channels can be very large. Synchronization can sometimes take several hours.

过程：可选：创建 Salt 状态以部署配置文件

1. 在 Uyuni 服务器 Web UI 上，导航到 **配置 > 通道**。

2. 单击 **[创建]**。

- 在 **名称** 字段中，键入 subscription-manager: disable yum plugins。
- 在 **别名** 字段中，键入 subscription-manager-disable-yum-plugins。
- 在 **描述** 字段中，键入 subscription-manager: disable yum plugins。
- 将 **SLS** **文件** 字段留空。

3. 单击 **[创建]**。

4. 单击 **[创建]**。

- 在 **路径** /etc/yum/pluginconf.d/subscription-manager.conf 字段中，键入 /etc/yum/pluginconf.d/subscription-manager.conf。
- 在 **值** 字段中，键入：

```
[main]
enabled=0
```

5. 单击 **[创建]**。

6. 记下 Salt **名称** 字段的值。

7. 单击配置通道的名称。

8. 单击 **'init.sls'**。

- 在 **值** 字段中，键入：

```
configure_subscription-manager-disable-yum-plugins:
cmd.run:
  - name: subscription-manager config
--rhsm.auto_enable_yum_plugins=0
  - watch:
    - file: /etc/yum/pluginconf.d/subscription-manager.conf
file.managed:
  - name: /etc/yum/pluginconf.d/subscription-manager.conf
  - source: salt:///etc/yum/pluginconf.d/subscription-
manager.conf
```

9. 单击 。



The Creating a Salt State to Deploy Configuration Files procedure is optional.

过程：为 Red Hat Enterprise Linux 客户端创建系统组

1. 在 Uyuni 服务器 Web UI 上，导航到 **系统 > 系统组**。
2. 单击 。
 - 在 **名称** 字段中，键入 `rhel-systems`。
 - 在 **别名** 字段中，键入 `RHEL`。
3. 单击 .
4. 单击 **常规** 选项卡。
5. 单击 **高级** 选项卡。
6. 在搜索框中键入 `subscription-manager: disable yum plugins`。
7. 单击  以查看状态。
8. 单击 **状态** 列中的状态对应的复选框。
9. 单击 .
10. 单击 .

If you already have RHEL systems added to Uyuni, assign them to the new system group, and then apply the highstate.

过程：将系统组添加到激活密钥

您需要修改用于 RHEL 系统的激活密钥，以包含之前创建的系统组。

1. 在 Uyuni 服务器 Web UI 上，导航到 **系统 > 激活密钥**。
2. 单击用于 RHEL 系统的每个激活密钥并：
3. 依次导航到 **-->** 选项卡和 **-->>** 子选项卡。

4. 选中 `rhel-systems`。
5. 单击 **[加入所选的组]**。

4.12.1.5. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。



对于 Red Hat 自定义通道，如果您要选中 `GPG URL` 字段，则需填充 `GPG URL` 字段。您可以使用 Red Hat 受控端 `/etc/pki/rpm-gpg` 目录下存储的 GPG 密钥的文件 URL。

示例：`file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release`

有关 Red Hat 产品签名密钥的完整列表，请参见 <https://access.redhat.com/security/team/key>。

4.12.1.6. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.12.2. Registering Red Hat Enterprise Linux clients with RHUI

This section contains information about using Red Hat update infrastructure (RHUI) to register clients running Red Hat Enterprise Linux operating systems.

If you are running clients in a public cloud, such as Amazon EC2, use this method.

可以将 RHUI 与 Red Hat 内容分发网络 (CDN) 搭配使用来管理您的 Red Hat Enterprise Linux 订阅。有关使用 Red Hat CDN 的信息，请参见 [Client-configuration > Clients-rh-cdn](#)。



您需负责将 Uyuni 服务器连接到 Red Hat 更新基础结构。所有使用此 RHUI 证书进行更新的客户端都需要获得正确许可，有关详细信息，请咨询您的云服务提供商，并查看服务的 Red Hat 条款。



当使用 RHUI 注册的 Red Hat Enterprise Linux 客户端关闭时，Red Hat 可能会声称证书无效。在此情况下，您需要再次打开客户端，或获取新的 RHUI 证书。

4.12.2.1. Import entitlements and certificates

In the past it was required to import the certificates and entitlement data manual into Uyuni Server. This task has been automated by using the same mechanism as for SUSE PAYG instances. For more information, see [Installation-and-upgrade > Connect-payg](#).

本指南将介绍注册到 Red Hat 更新基础结构 (RHUI) 的客户端。您至少须有一个注册到 RHUI 的系统并拥有授权订阅，以获得储存库内容。

而有关使用 Red Hat 内容分发网络 (CDN) 的信息，请参见 [Client-configuration > Clients-rh-cdn](#)。



要为客户端系统使用从属证书，必须有从属服务器和订阅。Uyuni 服务器不支持使用从属证书的客户端。



PAYG 连接会定期与客户端通讯以获取最新的身份验证数据。请务必保持客户端运行状态并定期更新。如果不这样，储存库同步有时将会失败，并显示身份验证错误。



请在连接任何 Red Hat 7 实例前先将其更新。



要连接到 Red Hat 9 实例，必须已为其配置加密策略 LEGACY。请执行 `sudo update-crypto-policies --set LEGACY` 进行相应配置。

4.12.2.2. 连接到 Red Hat 更新基础结构

过程：连接新的 Red Hat 实例

1. 在 Uyuni Web UI 中，导航到 **管理 > 安装向导 > PAYG**，然后单击 **[+]** [添加 PAYG]。
2. 从页面的 **PAYG** 部分开始。
3. 在 **说明** 字段中添加说明。
4. 转移到页面的 **SSH** 部分。
5. 在 **实例 DNS 或 IP 地址** 字段中，键入要从 Uyuni 连接的实例 DNS 或 IP 地址。
6. 在 **端口号** 字段中输入端口号或使用默认值 22。
7. 在 **用户名** 字段中输入云中指定的用户名。
8. 在 **口令** 字段中输入口令。
9. 在 **实例密钥** 字段中输入实例密钥。
10. 在 **密钥通行口令** 字段中输入密钥通行口令。



身份验证密钥必须采用 PEM 格式。

如果您要通过 SSH 堡垒连接实例而不是直接连接，请执行[过程：添加 SSH 堡垒连接数据](#)。

否则，请执行[过程：完成 Red Hat 连接](#)。

过程：添加 SSH 堡垒连接数据

1. 导航到页面的“**SSH 堡垒连接**”部分。
2. 在**主机名**字段中输入堡垒主机名。
3. 在**端口号**字段中输入堡垒端口号。
4. 在**用户名**字段中输入堡垒用户名。
5. 在**口令**字段中输入堡垒口令。
6. 在**密钥**字段中输入堡垒密钥。
7. 在**密钥通行口令**字段中输入堡垒密钥通行口令。

执行[过程：完成 Red Hat 连接](#)完成设置。

过程：完成 Red Hat 连接

1. 要完成添加新 Red Hat 连接数据的过程，请单击  [创建]。
2. 返回 PAYG 连接数据页面。顶部的“**连接**”部分会显示更新的连接状态。
3. **连接 > Red Hat > Pay-as-you-go** 屏幕中也会显示连接状态。
4. 如果实例的身份验证数据正确无误，**连接**列会显示“**已连接**”。



如果在任何时间输入了无效数据，**连接 > Red Hat > PAYG** 中会显示新创建的实例，同时**连接**列会显示错误消息。

当服务器上有可用的身份验证数据后，系统会立即为已连接实例上所有可用的储存库添加储存库。您可以在**连接 > Red Hat > 储存库**中查看储存库。



A Red Hat connection will create custom repositories which are owned by organization 1 by default. If a different organization should own the autogenerated repositories, configure `java.rhui_default_org_id` in `/etc/rhn/rhn.conf`.

此设置仅可定义和更新储存库。如果您想对受管客户端使用某个储存库，则需要指定软件通道并将储存库关联到该软件通道。

4.12.2.3. Add software channels

将 Red Hat 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 40. Red Hat 通道 - CLI

OS Version	Base Channel	Client Channel	Tools Channel
Red Hat 7	rhel7-pool-uyuni	-	rhel7-uyuni-client
Red Hat 8	rhel8-pool-uyuni	-	rhel8-uyuni-client
Red Hat 9	rhel9-pool-uyuni	-	rhel9-uyuni-client

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道。请确保指定正确的体系结构：

```
spacewalk-common-channels \
-a <体系结构> \
<基础通道名称> \
<子通道名称 1> \
<子通道名称 2> \
... <子通道名称 n>
```

2. 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <base_channel_label>-<architecture>
```

3. 确保同步已完成，然后再继续操作。



spacewalk-common-channels 提供的客户端工具通道来自 Uyuni 而非 SUSE。

4.12.2.4. Prepare custom channels

要从 RHUI 镜像软件，您需要在 Uyuni 中创建关联到自动生成的储存库的自定义通道。

此过程所需的通道包括：

表格 41. Red Hat 自定义通道

OS Version	Base Channel
Red Hat 7	rhel7-pool-uyuni
Red Hat 8	rhel8-pool-uyuni
Red Hat 9	rhel9-pool-uyuni

过程：创建自定义通道

1. 在 Uyuni 服务器 Web UI 上，导航到**软件**，**管理**，**通道**。
2. 单击 ，然后为通道设置相应的参数。
3. 在 **基础通道** 字段中，选择相应的基础通道。
4. 单击 。
5. 对需要创建的所有通道重复以上步骤。每个自定义储存库都应该有一个自定义通道。

您可以导航到**软件**，**通道列表**，**所有**，以检查是否已创建所有相应的通道和储存库。



对于 Red Hat 8 客户端，请添加基础通道和 AppStream 通道。您需要来自这两个通道的软件包。如果未添加这两个通道，将会因缺少软件包而无法创建引导储存库。

创建所有通道之后，可以将其与您创建的储存库关联：

过程：将通道与储存库关联

1. 在 Uyuni 服务器 Web UI 上，导航到**软件**，**管理**，**通道**，然后单击要关联的通道。
2. 导航到**储存库**选项卡，然后选中要与此通道关联的储存库。
3. 单击  以将通道与储存库相关联。
4. 对需要关联的所有通道和储存库重复以上步骤。
5. 可选：导航到**同步**选项卡，为此储存库设置定期同步日程安排。
6. 单击  以立即开始同步。

4.12.2.5. Check synchronization status

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到**同步**选项卡，然后单击**同步**并选中**立即同步**。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



Red Hat Enterprise Linux channels can be very large. Synchronization can sometimes take several hours.

4.12.2.6. Manage GPG keys

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。

4.12.2.7. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.13. Rocky Linux 客户端注册

您可以将 Rocky Linux} 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您必须已创建激活密钥。

- 有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。
- 有关将 Rocky Linux 迁移到 SUSE Liberty Linux 的详细信息，请参见 [client-configuration:clients-sleses.pdf](#)。

4.13.1. 注册 Rocky Linux 客户端

This section contains information about registering clients running Rocky Linux operating systems.



我们已使用----策略并采用默认的 SELinux 配置对将 Rocky Linux 客户端注册到 Uyuni 的过程进行了测试。将 Rocky Linux 客户端注册到 Uyuni 时，您无需禁用 SELinux。

4.13.1.1. 添加软件通道

将 Rocky Linux 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。

目前支持的系统结构有 x86_64 和 aarch64，在版本 9 上，另外还支持 ppc64le 和 s390x。有关支持的产品和体系结构的完整列表，请参见 [Client-configuration > Supported-features](#)。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 42. Rocky Linux 通道 - CLI

操作系统版本	基础通道	客户端通道	AppStream 通道
Rocky Linux 9	rockylinux9	rockylinux9-uyuni-client	rockylinux9-appstream
Rocky Linux 8	rockylinux8	rockylinux8-uyuni-client	rockylinux8-appstream

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道。请确保指定正确的体系结构：

```
spacewalk-common-channels \
-a <体系结构> \
<基础通道名称> \
<子通道名称 1> \
<子通道名称 2> \
... <子通道名称 n>
```

2. 如果 [自动同步](#) 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <base_channel_label>-<architecture>
```

3. 确保同步已完成，然后再继续操作。



`spacewalk-common-channels` 提供的客户端工具通道来自 Uyuni 而非 SUSE。



对于 Rocky Linux 8 和 Rocky Linux 9 客户端，请添加基础通道和 AppStream 通道。您需要来自这两个通道的软件包。如果未添加这两个通道，将会因缺少软件包而无法创建引导储存库。



您可能会发现 AppStream 通道中提供的软件包数量在上游通道和 Uyuni 通道之间存在一定的差异。如果您对在不同时间添加的同一通道进行比较，会发现其数量也不相同。这是由 Rocky Linux 管理其储存库的方式所致。当有新版本发布时，Rocky Linux 会去除软件包的较旧版本，而 Uyuni 则会保留所有版本，无论新旧与否。

If you are using modular channels with Rocky Linux 8, you must enable the Python 3.6 module stream on the client. If you do not provide Python 3.6, the installation of the `spacecmd` package will fail.

4.13.1.2. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到同步选项卡，然后单击同步并选中同步复选框。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。

4.13.1.3. 创建激活密钥

您需要创建与您的 Rocky Linux 通道关联的激活密钥。

有关激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.13.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。如果不信任 GPG 密钥，便无法为客户端指派软件通道。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。

4.13.1.5. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.13.1.6. 管理勘误

当您更新 Rocky Linux 客户端时，软件包会包含有关更新的元数据。

4.14. Ubuntu 客户端注册

您可以将 Ubuntu 客户端注册到 Uyuni 服务器。方法和细节视客户端的操作系统而异。

开始前，请确保客户端的日期和时间已与 Uyuni 服务器正确同步。

您还必须已创建好激活密钥。有关创建激活密钥的详细信息，请参见 [Client-configuration > Activation-keys](#)。

4.14.1. 注册 Ubuntu 20.04 和 22.04 客户端

This section contains information about registering clients running Ubuntu 20.04 LTS and 22.04 LTS operating systems.

支持使用引导功能启动 Ubuntu 客户端，并执行初始状态运行，例如设置储存库和执行配置文件更新。不过，默认会禁用 Ubuntu 上的 root 用户，因此要使用引导，需要有一个具有 Python sudo 特权的现有用户。



Canonical 未授权也不支持 Uyuni。

4.14.1.1. 添加软件通道

将 Ubuntu 客户端注册到您的 Uyuni 服务器之前，您需要添加所需的软件通道，并同步这些通道。



下面的小节中的说明通常默认使用 x86_64 体系结构。请根据情况将其替换为其他体系结构。

此过程所需的通道包括：

表格 43. Ubuntu 通道 - CLI

OS Version	Base Channel	Main Channel	Updates Channel	Security Channel	Client Channel
Ubuntu 22.04	ubuntu-2204-pool-amd64-uyuni	ubuntu-2204-amd64-main-uyuni	ubuntu-2204-amd64-main-updates-uyuni	ubuntu-2204-amd64-main-security-uyuni	ubuntu-2204-amd64-uyuni-client
Ubuntu 20.04	ubuntu-2004-pool-amd64-uyuni	ubuntu-2004-amd64-main-uyuni	ubuntu-2004-amd64-main-updates-uyuni	ubuntu-2004-amd64-main-security-uyuni	ubuntu-2004-amd64-uyuni-client

Version 20.04 also requires the Universe channels:

表格 44. Ubuntu 20.04 Universe Channels - CLI

Ubuntu 20.04	
Universe Channel	ubuntu-2004-amd64-universe-uyuni
Universe Updates Channel	ubuntu-2004-amd64-universe-updates-uyuni

Ubuntu 20.04	
Universe Security Updates Channel	ubuntu-2004-amd64-universe-security-uyuni
Universe Backports Channel	ubuntu-2004-amd64-universe-backports-uyuni

过程：在命令提示符处添加软件通道

1. 在 Uyuni 服务器上的命令提示符下，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道：

```
spacewalk-common-channels \
<基础通道标签> \
<子通道标签 1> \
<子通道标签 2> \
... <子通道标签 n>
```

2. 如果 **自动同步** 处于关闭状态，请同步通道：

```
spacewalk-repo-sync -p <基础通道标签>
```

3. 确保同步已完成，然后再继续操作。



在引导任何 Ubuntu 客户端之前，您需要完全同步所有新通道。

4.14.1.2. Mirror Ubuntu ESM packages

Canonical provides **Expanded Security Maintenance (ESM)** packages for **Ubuntu Pro** users and customers. These packages offer longer maintenance (10 to 12 years) for several operating system components and selected applications.

These repositories can also be synchronized within Uyuni if you extract the required **GPG keys** and your personal **Bearer Token** from a system registered to Ubuntu Pro.

4.14.1.2.1. Extract GPG keys and Bearer Token

Register an Ubuntu host with Ubuntu Pro. You will find your personal registration token in the **Ubuntu Pro Dashboard**. An **Ubuntu One account** is required for this.

```
sudo apt-get install ubuntu-adantage-tools
sudo pro attach <personal_token>
```

After registration, you will find the Bearer Token in the file `/etc/apt/auth.conf.d/90ubuntu-adantage`:

```
machine esm.ubuntu.com/apps/ubuntu/ login bearer password <token> #
ubuntu-pro-client
machine esm.ubuntu.com/infra/ubuntu/ login bearer password <token> #
ubuntu-pro-client
```



One dedicated bearer token is used per repository.

Configure the following repositories within Uyuni:

4.14.1.2.2. Configure Ubuntu ESM repositories

Use the following URLs for creating the repositories:

表格 45. Ubuntu ESM repositories

URL	Description
<a href="https://bearer:<token>@esm.ubuntu.com/infra/ubuntu/dists/<release>-infra-updates/main/binary-<arch>/">https://bearer:<token>@esm.ubuntu.com/infra/ubuntu/dists/<release>-infra-updates/main/binary-<arch>/	Operating system functional updates
<a href="https://bearer:<token>@esm.ubuntu.com/infra/ubuntu/dists/<release>-infra-security/main/binary-<arch>/">https://bearer:<token>@esm.ubuntu.com/infra/ubuntu/dists/<release>-infra-security/main/binary-<arch>/	Operating system security updates
<a href="https://bearer:<token>@esm.ubuntu.com/apps/ubuntu/dists/<release>-apps-updates/main/binary-<arch>/">https://bearer:<token>@esm.ubuntu.com/apps/ubuntu/dists/<release>-apps-updates/main/binary-<arch>/	Application functional updates
<a href="https://bearer:<token>@esm.ubuntu.com/apps/ubuntu/dists/<release>-apps-security/main/binary-<arch>/">https://bearer:<token>@esm.ubuntu.com/apps/ubuntu/dists/<release>-apps-security/main/binary-<arch>/	Application security updates

Replace `<token>` with your personal Bearer Token. Also, `arch` and `release` must be replaced with one of the following values:

表格 46. Ubuntu ESM architectures and releases

Architectures	Releases
amd64, arm64, armel, armhf, i386, powerpc, ppc64el, s390x	bionic, focal, jammy, noble, trusty, xenial

In order for Uyuni to synchronize the repositories, the corresponding GPG keys (`ubuntu-advantage-esm-infra-trusty.gpg`, `ubuntu-advantage-esm-apps.gpg`) must be imported. These are located on a system registered with Ubuntu Pro under `/etc/apt/trusted.gpg.d`. Copy these files to the Uyuni system and import them as follows:

```
mgradm gpg add /path/to/gpg.key
```

Create the appropriate child channels below already synchronized Ubuntu parent channels. After that, repositories can be synchronized.



The procedure shown here can be used to circumvent the subscription limitations - however, this constitutes a breach of the Terms of Service and may have **legal consequences**. There must always be sufficient subscriptions for the number of systems used.

4.14.1.3. 检查同步状态

过程：在 Web UI 中检查同步进度

1. 在 Uyuni 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。
2. 导航到同步选项卡，然后单击并选中。

过程：在命令提示符处检查同步进度

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 tail 命令检查同步日志文件：

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

2. 每个子通道在同步过程中都会生成自己的日志。您需要检查所有基础通道和子通道日志文件，以确保同步已完成。



Ubuntu 通道可能会非常大。同步所需的时间可能会长达数小时。

4.14.1.4. 管理 GPG 密钥

安装软件包之前，客户端会使用 GPG 密钥检查这些软件包的真实性。只有可信软件才能安装在客户端上。



信任 GPG 密钥对于客户端的安全非常重要。由管理员来决定需要哪些密钥，可以信任哪些密钥。这是因为如果不信任 GPG 密钥，便无法使用软件通道，是否将通道指派给客户端取决于是否信任密钥。

有关 GPG 密钥的详细信息，请参见 [Client-configuration > Gpg-keys](#)。

4.14.1.5. Root 访问权限

默认会为 Ubuntu 上的 root 用户禁用 SSH 访问权限。

要想能够使用普通用户进行初始配置，您需要编辑 sudoers 文件。



This issue happens with self-installed versions of Ubuntu. If the default user has been granted administrative privileges during installation time, a password is required to perform privilege escalation using `sudo`. With cloud instances this does not happen because `cloud-init` automatically creates a file under `/etc/sudoers.d` and grants privilege escalation through `sudo` without the need for a password.

过程：向 Root 用户授予访问权限

- 在客户端上，编辑 `sudoers` 文件：

```
sudo visudo
```

在 `sudoers` 文件末尾添加下面一行，以向用户授予 `sudo` 访问权限。以在 Web UI 中引导客户端的用户的名称替换 `<user>`：

```
<user>  ALL=NOPASSWD: /usr/bin/python, /usr/bin/python2,  
/usr/bin/python3, /var/tmp/venv-salt-minion/bin/python
```



此过程无需口令便可授予 `root` 访问权限，而注册客户端需要提供口令。客户端成功安装后会以 `root` 特权运行，因此将不再需要该访问权限。客户端成功安装之后，建议您从 `sudoers` 文件中去除该行。

4.14.1.6. 注册客户端

要注册您的客户端，需要有引导储存库。默认会自动创建引导储存库，并且每天会为所有同步的产品重新生成该储存库。您可以在命令提示符处使用以下命令手动创建引导储存库：

```
mgr-create-bootstrap-repo
```

有关注册客户端的详细信息，请参见 [Client-configuration > Registration-overview](#)。

4.15. Client Registration to a Proxy

Proxy servers can act as a broker and package cache for clients. Registering clients to a proxy is similar to registering them directly to the Uyuni Server, with a few key differences.

These sections contain information on registering clients to a proxy using the Web UI, commands on the command line, or a bootstrap script. There are also procedures how you can move clients from one Uyuni Proxy to another one or to the Uyuni Server.

Within the Web UI, proxy pages show information about clients. You can see a list of clients that are connected to a proxy by clicking the name of the proxy in **Systems > System List > Proxy**, then select the

Proxy subtab of the Details tab.

A list of chained proxies for a client can be seen by clicking the name of the client in **Systems > All**, then select the Connection subtab of the Details tab.

4.15.1. Move Clients Between Proxies

You can move clients (Salt) and Salt SSH push clients between proxies without the need to repeat the registration process.



链式代理无法移动。您应创建新代理，移动客户端，然后删除旧代理，而不是移动链式代理。

Procedure: Moving Clients or Salt SSH Push Client Between Proxies

1. 在 Uyuni Web UI 中，导航到要在代理之间移动的客户端的-----页面。
2. 导航到----选项卡，然后单击-----链接，您会看到下拉菜单。
3. 在-----下拉菜单中，选择要移动到的目标代理，然后单击 [更改代理]。

Procedure: Moving Multiple Clients or Salt SSH Push Clients Between Proxies with SSM

1. 在 Uyuni Web UI 中，导航到**系统**，**系统列表**，然后选中要移动的每个客户端，如此会将这些客户端添加到系统集管理器中。
2. 导航到**系统**，**系统集管理器**，然后转到**其他**，**代理**选项卡。
3. 在-----下拉菜单中，选择要将客户端移动到的目标代理，然后单击 [更改代理]。

通过调用 `system.changeProxy` 也能使用该功能。

4.15.1.1. 背景信息

此功能对常规 Salt 客户端与 Salt SSH Push 客户端的作用有所不同。

4.15.1.1.1. Default Clients

The function schedules a Salt state action, which modifies `master:` setting in the `susemanager.conf` Salt client configuration file to point to the new proxy. Then the function restarts the Salt client.



通过手动编辑 `susemanager.conf` 文件来更改 `master:` 也有同样的效果，并且系统也支持这种方式。

When the client restarts and reconnects via the new proxy, the server updates the proxy path in the database and schedules another action for refreshing the channel URLs.

4.15.1.1.2. Salt SSH Push Clients

该功能会立即在数据库中更新代理路径并安排新操作来刷新通道 URL。

4.15.2. 将客户端从代理移到服务器

If you want to move a client from a proxy to the server, select **None** from proxy list.

4.15.3. 使用 Web UI 将客户端注册到代理

You can register clients to the Uyuni Proxy using the Web UI.

A bootstrap repository is needed for non-SLE clients in general and for SLE clients before version 15.

For information about creating a bootstrap repository, see [Client-configuration > Bootstrap-repository](#).

过程：使用 Web UI 将客户端注册到代理

1. 在 Uyuni Web UI 中，导航到 **系统 > 引导**。
2. 在 **引导 URL** 字段中，键入要引导的客户端的完全限定域名 (FQDN)。
3. 在 **SSH 端口号** 字段中，键入用于连接和引导客户端的 SSH 端口号。SSH 端口默认为 22。
4. 在 **用户名** 字段中，键入用于登录客户端的用户名。用户名默认为 `root`。
5. 在 **身份验证方法** 字段中，选择用于引导客户端的身份验证方法。
 - 如果选择的是口令身份验证，请在 **口令** 字段中，键入用于登录客户端的口令。
 - 如果选择的是 SSH 私用密钥身份验证，请输入私用密钥和关联的通行口令。该密钥的存储期截止到引导过程完成。
6. 在 **激活密钥** 字段中，选择与您要用于引导客户端的软件通道关联的激活密钥。
7. 在 **代理服务器** 字段中，选择要注册到的代理服务器。
8. 默认会选中 **自动接受 SSH 主机密钥** 复选框。如此可让引导过程自动接受 SSH 主机密钥，而无需您手动进行身份验证。
9. 可选：选中 **仅使用 SSH 连接** 复选框。如果您选中此选项，客户端将会配置为使用 SSH 来连接服务器，且不再配置其他连接方法。
10. 单击 **[Bootstrap]** 开始注册。

引导过程完成时，您的客户端即会列在 **系统 > 系统列表** 中。

4.15.4. Register Clients on the Command Line

Instead of the Web UI, you can use the command line to register a client to a proxy. This procedure requires that you have installed the Salt package on the client before registration. For SLE 12 based clients, you also must have activated the Advanced Systems Management module.

过程：使用命令行将客户端注册到代理

1. 选择位于以下位置的客户端配置文件：

```
/etc/salt/minion
```

或：

```
/etc/salt/minion.d/NAME.conf
```

该文件有时也称为受控端文件。

- 将代理 FQDN 作为 master 添加到客户端配置文件：

```
master: PROXY123.EXAMPLE.COM
```

- 重启 salt-minion 服务：

```
systemctl restart salt-minion
```

- 在服务器上，接受新客户端密钥（将 <client> 替换为您客户端的名称）：

```
salt-key -a '<client>'
```

4.16. Registering Clients on a Public Cloud

设置好 Uyuni 服务器后，您便可开始注册客户端。

4.16.1. 添加产品并同步储存库

确保您已添加客户端的对应产品并已将储存库同步到 Uyuni。要创建用于注册客户端的引导储存库，必须执行此操作。

For more information, see [Specialized-guides > Public-cloud-guide](#).

4.16.2. Prepare On-demand Images

使用 SUSE 提供的按需映像开始的实例会自动进行注册，并且更新基础结构和 SUSE Linux Enterprise 模块均已激活。要使用按需映像作为 Uyuni 客户端，您需要在开始前禁用此自动功能。

Procedure: Preparing On-demand Images

- 登录到按需实例。
- 在命令提示符处，以 root 身份去除注册数据和储存库：

```
registercloudguest --clean
```

3. 去除自动注册的触发服务。

```
systemctl disable guestregister.service
```

4. in Microsoft Azure, there is an additional service that needs to be disabled:

```
systemctl disable regionsrv-enabler-azure.timer
```

4.16.3. 注册客户端

在 Uyuni Web UI 中，导航到 **系统 > 引导**，然后填写 **名称**、**SSH 密钥**、**用户名** 和 **密码** 字段。请确保为 **名称** 字段使用稳定的 FQDN，否则，如果公有云为您分配一个不同的临时 FQDN，Uyuni 将找不到您的主机。

公有云映像通常不允许使用用户名和口令进行 SSH 登录，仅允许通过证书进行 SSH 登录。如果您要从 Web UI 中使用引导，则需启用通过用户名和 SSH 密钥进行 SSH 登录的功能。您可以通过导航到 **系统 > 引导** 并更改身份验证方法来启用此功能。

如果您的云提供商是 Microsoft Azure，您可以通过用户名和口令登录。要实现此目的，您需要允许 AzureUser 以 root 身份无口令运行命令。为此，请打开 `/etc/sudoers.d/waagent` 文件，并添加或编辑下面一行：

```
AzureUser ALL=(ALL) NOPASSWD: ALL
```



允许 AzureUser 以 root 身份无口令运行命令会带来安全风险。请仅将此方法用于测试目的，不要用于生产系统。

引导过程成功完成时，您的客户端即会列在 **系统 > 系统列表** 中。

- If you want more control over the process or have to register many clients, create a bootstrap script. For more information, see **Client-configuration > Registration-bootstrap**.
- 如果要注册 Salt 客户端而且想更好地控制注册过程，在命令行上执行单个命令较为合适。有关详细信息，请参见 **Client-configuration > Registration-cli**。
- 注册从公有云映像（例如 AWS AMI）启动的客户端时，需要进行额外的配置以防它们彼此重写。有关注册克隆客户端的详细信息，请参见 **Administration > Troubleshooting**。

4.16.4. 激活密钥

Activation keys are used to ensure that your clients have the correct software entitlements, are connecting to the appropriate channels, and are subscribed to the relevant groups. Each activation key

is bound to an organization, which you can set when you create the key.

有关激活密钥的详细信息，请参见 **Client-configuration > Activation-keys**。

4.16.5. 自动注册 Terraform 创建的客户端

Terraform 创建的新客户端可以自动注册到 Uyuni 中。可以通过以下两种方式来完成注册：

- 基于 cloud-init 的注册
- 基于 remote-exec 置备器的注册

4.16.5.1. cloud-init Based Client Registration

自动注册新创建的虚拟机的首选方式是利用 cloud-init 进行注册。采用这种方法无需配置与主机的 SSH 连接。此外，无论使用哪种工具创建客户端，都可以采用这种方法。

用户可以在使用 Terraform 部署映像时传递用户数据集，以便将虚拟机自动注册到 Uyuni 中。`user_data` 只会在虚拟机首次启动时的引导期间运行一次。

使用 cloud-init 注册客户端之前，用户必须配置：

- 引导脚本。有关详细信息，请参见 **Client-configuration > Registration-bootstrap**。
- 激活密钥。有关详细信息，请参见 **Client-configuration > Activation-keys**。

下面的命令会下载引导脚本并在新虚拟机创建后注册该虚拟机。应将此命令添加到 cloud-init 配置中：

```
curl -s http://hub-server.tf.local/pub/bootstrap/bootstrap-default.sh |  
bash -s
```



Any time `user_data` is updated to change the provisioning, Terraform will destroy and then recreate the machines with a new IP, etc.

有关 AWS 上的 cloud-init 的详细信息，请参见 https://registry.terraform.io/providers/hashicorp/template/latest/docs/data-sources/cloudinit_config。

有关 cloud-init 示例，请参见 https://registry.terraform.io/providers/hashicorp/cloudinit/latest/docs/data-sources/cloudinit_config#example-usage。

4.16.5.2. remote-exec Provisioner Based Registration

第二种自动注册新创建的虚拟机的方法是使用 Terraform 的 remote-exec 置备器。

remote-exec 置备器会与新创建的虚拟机进行交互。它会建立 SSH 连接，然后便可对该虚拟机上运行命令。



使用 `remote-exec` 置备器注册客户端时，用户必须确保运行 Terraform 的虚拟机在新虚拟机创建后可以访问该虚拟机。

其他要求与使用 [cloud-init Based Client Registration](#) 时相同：

- 引导脚本。有关详细信息，请参见 [Client-configuration > Registration-bootstrap](#)。
- 激活密钥。有关详细信息，请参见 [Client-configuration > Activation-keys](#)。

下面的命令会下载引导脚本并在新虚拟机创建后注册该虚拟机。应将此命令定义为要运行的远程命令：

```
curl -s http://hub-server.tf.local/pub/bootstrap/bootstrap-default.sh |  
bash -s
```

有关 `remote-exec` 置备器的详细信息，请参见 <https://www.terraform.io/docs/provisioners/remote-exec.html>。

Chapter 5. 客户端升级

客户端采用底层操作系统的版本控制系统，需要定期升级。

For SCC registered clients using SUSE operating systems, you can perform upgrades within the Uyuni Web UI. For supported SUSE Linux Enterprise 15 upgrade paths, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-upgrade-paths.html>

将运行 SLE 12 的客户端升级到 SLE 15 的过程可自动完成，不过在开始前您需要完成一些准备步骤。有关详细信息，请参见 **Client-configuration** > **Client-upgrades-major**。

您也可以使用内容生命周期管理器自动执行客户端升级。有关详细信息，请参见 **Client-configuration** > **Client-upgrades-lifecycle**。

For more information about product migration such as service pack upgrades, openSUSE Leap minor version upgrades, or openSUSE Leap to SUSE Linux Enterprise migrations, see **Client-configuration** > **Client-upgrades-product-migration**.

有关激活密钥的详细信息，请参见 **Client-configuration** > **Activation-keys**。

5.1. Major Version Upgrade

The clients must have the latest available service pack (SP) for the installed operating system, with all the latest updates applied. Before you start, ensure that the system is up to date and all updates have been installed successfully.

升级由 YaST 和 AutoYaST 控制，该过程不使用 Zypper。

5.1.1. Prepare to Migrate

Before you can migrate your client from SLE 12 to SLE 15, you need to:

1. 准备安装媒体
2. Declare an autoinstallation distribution
3. 创建激活密钥
4. 创建自动安装配置文件

5.1.1.1. Prepare Installation Media

Procedure: Preparing Installation Media

1. On the container host, download an ISO image with the installation sources.
2. Use `mgradm` to import the installation data from the ISO image:

```
mgradm distribution copy <image_name>.iso <image_name>
```

3. Take a note of the distribution path reported by `mgradm`. You will need it when you declare the distribution to Uyuni.



This image can be used for multiple autoinstallation distributions.

有关详细信息，请参见 [Client-configuration > Autoinst-distributions](#)。

5.1.1.2. Declare an Autoinstallation Distribution

Procedure: Declaring an Autoinstallation Distribution

1. 在 Uyuni Web UI 中，导航到系统，自动安装，发行套件。
2. Click `Create Distribution`, and complete these fields:

In the `Distribution Label` field, enter a name to identify your autoinstallation distribution. For example, `sles15sp6-x86_64`. * In the `Tree Path` field, enter the path to the installation media you already saved. * Select the matching `Base Channel`. This must match the installation media. * Select the `Installer Generation`. This must match the installation media. * OPTIONAL: Specify kernel options to use when booting this distribution. There are multiple ways to provide kernel options. Only add options here that are generic for the distribution.

3. Click `Create Autoinstallable Distribution`.

5.1.1.3. 创建激活密钥

For example, to switch from the old SLE 12 base channel to the new SLE 15 channel, you need an activation key.

过程：创建激活密钥

1. 在 Uyuni 服务器 Web UI 中，导航到系统，激活密钥，然后单击 `-----`。
2. 输入密钥说明。
3. 输入密钥或将其留空以生成自动密钥。
4. 可选：如果您要限制使用次数，请在 `----` 文本字段中输入值。
5. Select the `SLE-Product-SLES15-SP6-Pool` for `x86_64` base channel.
6. 可选：选择任何 `-----`。For more information, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/article-modules.html>.
7. 单击 `[创|建|激|活|密|钥]`。
8. 单击 `-----` 选项卡，然后选择所需通道。
9. 单击 `[更|新|密|钥]`。

5.1.1.4. 创建自动安装配置文件

自动安装配置文件包含安装系统所需的所有安装和配置数据，还包含在完成安装后需要执行的脚本。例如，可用作着手点的脚本，请参见 <https://github.com/SUSE/manager-build-profiles/tree/master/AutoYaST>。

For valid AutoYaST upgrade settings, see <https://doc.opensuse.org/projects/autoyast/#CreateProfile-upgrade>.

过程：创建自动安装配置文件

1. 在 Uyuni Web UI 中，导航到系统，自动安装，配置文件，然后上载自动安装配置文件脚本。

For example scripts that you can use as a starting point, see:

<https://github.com/SUSE/manager-build-profiles/tree/master/AutoYaST>。

2. 在……字段中，键入 autoupgrade=1。

(可选) 您也可以包含 Y2DEBUG=1 选项。调试设置不是必需的设置，不过此设置有助于对您未来可能遇到的任何问题进行查错。



在 Azure 云中运行的客户端必须将 textmode=1 console=ttyS0 添加到……中。

3. 粘贴自动安装配置文件或使用文件上载字段。

4. 单击 [创建] 保存设置。

5. 如果需要为上载的配置文件设置变量，请导航到系统，自动安装，配置文件，选择要编辑的配置文件，然后导航到……选项卡。

使用以下格式指定所需的变量：

```
<key>=<value>
```

5.1.2. 迁移

在开始前，需检查自动安装配置文件中引用的所有通道是否可用并已完全同步。

您可以在 /var/log/rhn/reposync/<channel-label>.log 中监控镜像进度。

过程：迁移

1. 在 Uyuni 服务器 Web UI 中，导航到……，然后选择要升级的客户端。
2. 导航到……选项卡，然后选择上载的自动安装配置文件。
3. 单击 [安排] [自动] [安] [装] [并] [完] [成]。系统会下载所需的文件，更改引导加载程序项，重引导并开始升级。

客户端下次与 Uyuni 服务器同步时，会收到重新安装作业。重新安装作业会提取新内核和 initrd 软件包，还会写入新的 /boot/grub/menu.lst (GRUB Legacy) 或 /boot/grub2/grub.cfg (GRUB 2)，包含指向新内核和 initrd 软件包的指针。

客户端下次引导时，会使用 grub 来引导新内核及其 initrd。此过程中不会使用 PXE 引导。

提取作业约 3 分钟后，客户端会关闭以重引导。



For clients, use the `spacewalk/minion_script` snippet to register the client again after migration has completed.

5.2. 使用内容生命周期管理器升级

如果您需要管理的 SUSE Linux Enterprise Server 客户端有很多，可以使用内容生命周期管理器自动执行就地升级。

5.2.1. 准备升级

升级客户端之前，需要完成以下准备工作：

- 创建内容生命周期项目
- 创建激活密钥
- 创建可自动安装的发行套件
- 创建自动安装配置文件

过程：创建内容生命周期项目

1. 为您的发行套件创建内容生命周期项目。

有关详细信息，请参见 **Administration > Content-lifecycle**。

2. 务必为您的项目选择简短的非描述性名称。
3. 添加您的发行套件所需的所有源通道模块。
4. 视需要添加过滤器，并至少设置一个环境。

过程：创建激活密钥

1. 为您的发行套件创建激活密钥。

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

2. 确保您的激活密钥包含所有过滤出的项目通道。

过程：创建可自动安装的发行套件

1. 为要迁移的每个基础通道创建可自动安装的发行套件。

有关详细信息，请参见 **Client-configuration > Autoinst-distributions**。

2. 为您的发行套件指定一个标签来表示内容生命周期项目的名称。
3. 在-----字段中，选择要使用的 SLES 版本。

过程：创建自动安装配置文件

1. 为要升级到的每个目标发行套件和服务包创建自动安装配置文件。

有关详细信息，请参见 **Client-configuration > Autoinst-profiles**。

2. 您可以在配置文件中使用变量来区分不同的生命周期环境。

有关自动安装配置文件的示例，请参见 <https://github.com/SUSE/manager-build-profiles/tree/master/AutoYaST>。

在自动安装配置文件中使用以下变量来实现自动就地升级：

列表 1. 例如：在自动安装配置文件中使用的变量

```
registration_key=1-15sp1-demo-test
org=1
channel_prefix=15sp1-demo-test
distro_label=15sp1-demo-test
```

列表 2. 例如：在自动安装配置文件中使用的项

```
<listentry>
  <ask_on_error config:type="boolean">true</ask_on_error>

  <media_url>https://$redhat_management_server/ks/dist/child/$channel_prefix-sle-module-web-scripting15-sp1-pool-x86_64/$distro_label</media_url>
    <name>$channel_prefix SLE-Module-Web-Scripting15-SP1 Pool for x86_64
  </name>
    <product>Web Scripting Module 15 SP1 x86_64 Pool</product>
</listentry>
```

5.2.2. 升级

准备好要升级的服务器后，您便可置备客户端。

过程：置备客户端

1. 在 Uyuni Web UI 中，导航到**系统 > 系统列表**，选择要置备的客户端，以将其添加到系统集管理器中。
2. 导航到**系统 > 系统集管理器 > 概览**，然后单击“选项卡”。
3. 选择要使用的自动安装配置文件。

对于可以使用 PXE 的客户端，当您完成置备后，客户端便会立即自动迁移。对于所有其他客户端，您可以使用 Cobbler 来执行升级。

过程：使用 Cobbler 升级客户端

1. At the command prompt, as root, to get to a shell inside the container, run:

```
mgrctl term
```

1. Check the available Cobbler profiles:

```
cobbler profile list
```

2. 使用您选择的配置文件和发行套件构建 ISO 文件:

```
cobbler buildiso --iso=/tmp/SLE_15-sp1.iso --profiles=SLE_15-sp1:1:Example --distro=SLE_15-sp1
```

有关使用 CD-ROM 置备客户端的详细信息, 请参见 [Client-configuration > Autoinst-cdrom](#)。

5.3. 产品迁移

通过产品迁移, 您可以将基于 SLE 的客户端系统从服务包 (SP) 级别升级到更高级别。例如, 您可以将 SUSE Linux Enterprise Server 15 SP1 升级到 SUSE Linux Enterprise Server 15 SP2。

产品迁移用于在同一主要版本内升级。您无法通过产品迁移从 SUSE Linux Enterprise Server 12 迁移到 SUSE Linux Enterprise Server 15。有关主要升级的详细信息, 请参见 [Client-configuration > Client-upgrades-major](#)。

您还可以将 openSUSE Leap 迁移到更高的次要版本或对应的 SUSE Linux Enterprise Server SP 级别, 例如:

- openSUSE Leap 15.1 to 15.2
- openSUSE Leap 15.1 to SUSE Linux Enterprise Server 15 SP1
- 将 openSUSE Leap 15.5 迁移到 SUSE Linux Enterprise Server 15 SP5

在 SUSE Linux Enterprise Server 12 及更高版本中, SUSE 支持跳过服务包 (如果 SUSE Customer Center 提供该服务包)。例如, 您可以从 SUSE Linux Enterprise Server 15 升级到 SP2, 而无需安装 SP1。

For supported SUSE Linux Enterprise Server upgrade paths, see <https://documentation.suse.com/en-us/sles/15-SP4/html/SLES-all/cha-upgrade-paths.html#sec-upgrade-paths-supported>.



迁移期间, Uyuni 会在安装前自动接受任何必要的许可协议 (EULA)。

5.3.1. 单系统迁移

开始迁移产品之前:

- 确保没有待处理更新或补丁。请检查客户端系统 [细节](#) > [概览](#) 页面上的 , 然后安装提供的所有

更新或补丁。如果您的客户端系统不是最新的，产品迁移可能会失败。

- 确保目标产品的所有通道都已完全同步。要在 Web UI 中检查同步状态，请导航到管理，安装向导，产品页面。
- 请确保您具有有效的系统备份，以防万一。产品迁移没有回滚功能。迁移过程一旦开始，就无法回滚。

过程：执行单系统迁移

- 从系统，概览页面中，选择一个客户端。
- 从客户端的系统细节页面，导航到软件，产品迁移选项卡。
- 选择目标迁移路径，然后单击 **[选择通道]**。
- 从 **基础通道** - **基础** 页面选择正确的基础通道，包括 **基础** 和任何其他 **基础**。
- 可选：选中 **允许安装供应商发生更改的软件包**，以允许安装供应商发生更改的软件包。如果发生此情况，开始迁移前会显示一条包含相关细节的通知。



要将 openSUSE Leap 迁移到 SUSE Linux Enterprise Server，必须选中 **基础** 选项。

- 正确配置您的通道后，单击 **[安排迁移]**。

5.3.2. 产品大量迁移

如果您要将大量客户端迁移到下一 SP 版本，可以使用 Uyuni API 调用。

spacecmd 命令行工具提供了 system_scheduleproductmigration 子命令，可用于安排将大量客户端迁移到下一次要版本。

5.3.2.1. 执行产品大量迁移



产品大量迁移操作非常危险，该过程应经过全面测试。至少应先进行试运行。

请务必小心，不要无意中升级系统。

过程：执行产品大量迁移

- 列出可用的迁移目标，并记下要迁移的系统 ID：

```
spacecmd api -- system.listMigrationTargets -A 1000010001
```

- 针对每个系统 ID 调用 listMigrationTarget，并查看所需的目标产品是否可用。

- 如果系统 ID 有可用目标，则调用 system. scheduleProductMigration。
- 如果所需目标不可用，则跳过该系统。

- 根据您的环境调整以下模板：

```

target = '[....]'
basechannel = 'channel-label'
system_ids = [1, 2, 3]

session = auth.login(user, pass)
for system in system_ids
    if system.listMigrationTargets(session, system).ident == target
        system.scheduleProductMigration(session, system, target,
basechannel, [] , False, <now>)
    else
        print "无法迁移到请求的目标 -- 正在跳过系统"
    endif
endfor

```

5.3.2.2. 示例：从 SLES 15 SP2 迁移到 SLES 15 SP3

对于此示例，将会创建一个组，以便于进行大量迁移。

过程：创建大量产品迁移组

1. 在 Uyuni Web UI 中，导航到 **系统** > **系统组**，然后单击 **[创建组]**。
2. 将该组命名为 `mpm-target-sles15sp3`。
 - 您应该仅将订阅了相同基础通道的系统添加到创建的组中。本示例只会将订阅了 `SLE-Product-SLES15-SP2-Pool for x86_64` 的系统添加到该组中。

For more information about adding clients to groups, see **Client-configuration** > **System-groups**.

过程：将系统添加到组

1. 运行以下命令，以获取该组中所有系统的 ID：

```
spacecmd -- system_listmigrationtargets group:mpm-target-sles15sp3
```

2. 命令的输出为由多个 ID 组成的字符串。
 - 请只选择一个目标，这样所有系统报告的就是该目标。
 - 该字符串是另一个命令的 MIGRATIONTARGET 的标识符。



spacecmd 的子命令 system_scheduleproductmigration 和 system_listmigrationtargets 会遍历该组中的所有系统。

If there are 100 systems in the group, you will see 100 actions scheduled.

该组中的所有系统都必须支持相同的迁移目标。

过程：运行大量迁移命令

1. system_scheduleproductmigration 命令的语法如下：

```
spacecmd -- system_scheduleproductmigration <SYSTEM>
<BASE_CHANNEL_LABEL> \
<MIGRATION_TARGET> [选项]
```

2. 对于此示例，要将 mpm-target-sles15sp3 组中的所有系统从 SLES 12 SP2 升级到 SLES 15 SP3，请在命令行上输入以下命令：

```
spacecmd -- system_scheduleproductmigration group:mpm-target-
sles15sp3 \
sle-product-sles15-sp3-pool-x86_64 "[190,203,195,1242]" -d
```

5.3.2.2.1. 命令语法说明

要查看 system_scheduleproductmigration 的语法和选项，请运行以下命令：

```
spacecmd system_scheduleproductmigration help
```

<SYSTEM>

对于此示例，我们将使用我们创建的组选择该组中的所有系统：

```
group:mpm-target-sles15sp3
```

<BASE_CHANNEL_LABEL>

这是目标基础通道的标签。在本例中，系统将升级到 SLES 15 SP3，且标签为 sle-product-sles15-sp3-pool-x86_64。

要查看当前镜像的所有基础通道的列表，请运行以下命令：

```
spacecmd softwarechannel_listbasechannels
```

请注意，除非通道是当前基础通道的可用目标，否则您无法升级到该通道。

<MIGRATION_TARGET>

要为 group:mpm-target-sles15sp3 组中的系统确定此值，请运行以下命令：

```
spacecmd -- system_listmigrationtargets group:mpm-target-sles15sp3
```

必须采用以下格式传递 MIGRATION_TARGET 参数；请注意需要使用引号将其括住以防中括号会产生问题：
：

```
"[190,203,195,1242]"
```

选项

- -s START_TIME
- -d 如果您要执行试运行，请传递此标志（建议在实际执行迁移前执行试运行）
- -c CHILD_CHANNELS（逗号分隔的子通道标签（不带空格））

在本例中，我们包含了 -d 选项，在成功执行试运行后可以将其去除。

如果成功，安排的每个系统的命令输出将如下所示：

```
正在为以下系统安排产品迁移 mpm-sles152-1  
已安排操作 ID: 66
```

You can also track the action, in this case the dry run, in the Web UI for a given system in the group. From the system details page of the client, navigate to **Events > History**. If there are any failures during the dry run, the system should be investigated.

If all is well, the -d option can be removed from the command to run the real migration. After the migration is complete, you can reboot the system from the Uyuni Web UI.

5.4. 升级 Uyuni 客户端

在本节中，我们以 openSUSE Leap 为例。

5.4.1. 准备升级

过程：准备客户端升级

- 在 Uyuni 服务器上的命令提示符处，以 root 身份使用 `spacewalk-common-channels` 命令添加相应的通道。

```
spacewalk-common-channels \
opensuse_leap15_4 \
opensuse_leap15_4-non-oss \
opensuse_leap15_4-non-oss-updates \
opensuse_leap15_4-updates \
opensuse_leap15_4-uyuni-client
```

- 使用 `spacewalk-repo-sync` 完全同步所有通道。对于已定义的储存库 URL，继续 [installation-and-upgrade:proxy-uyuni.pdf](#)。
- 在 Uyuni 服务器 Web UI 中，导航到软件 > 管理 > 通道，然后单击 `Uyuni Client Tools for openSUSE Leap 15.4 (x86_64)` 通道名称。
- 在右上角单击 。
- 单击  选项卡，然后选择 `- Uyuni Client Tools for openSUSE Leap 15.3 (x86_64)`。
- 单击 。
- 对 `openSUSE Leap 15.4 (x86_64)` 和 `- openSUSE Leap 15.3 (x86_64)` 执行相同的操作。

展开 `openSUSE Leap 15.4 (x86_64)` 以查看填充了软件包的所有子通道。

5.4.2. 升级

要升级客户端，您需要替换软件储存库，然后更新软件，最后重引导客户端。

过程：升级客户端

- 在 Uyuni 服务器 Web UI 中，导航到系统，然后单击客户端的名称。
- 单击软件 > 软件通道，选择 `openSUSE Leap 15.5` 列表中所列的 `openSUSE Leap 15.5` 通道作为基础通道。
- 在 `子通道` 窗格中，选择 `15.5` 子通道。
- 单击 ，然后单击  以 `完成`。
- 单击 `升级软件包`，选择客户端上要更新的所有软件包，然后应用选择。单击 ，查看细节，然后单击  以完成更新。
- 重引导客户端。

如果需要更新许多客户端，可以在 Uyuni 服务器上创建由此命令序列组成的操作链。您可以使用操作链同时对多个客户端执行更新。

Chapter 6. 客户端删除

If you need to remove a client from your Uyuni Server, you can:

- use the Web UI to delete it
- remove a client from the command line.

6.1. 使用 Web UI 删除客户端

过程：删除客户端

1. 在 Uyuni Web UI 中，导航到 **系统** > **系统列表**，然后选择要删除的客户端。
2. 单击 。
3. 检查细节并单击 确认。
4. 对于 Salt 客户端，Uyuni 会尝试清理其他配置。如果无法联系客户端，您可以选择取消删除，或者仅删除客户端而不清理配置文件。

You can also delete multiple clients using the System Set Manager. For more information about the System Set Manager, see [Client-configuration](#) > [System-set-manager](#).



Cleaning up a client only disables Salt and stops the service if possible. It does not uninstall the package.

6.2. Delete a Client on the Command Line (with API Call)

过程：从服务器上删除客户端

1. 使用 FQDN（完全限定的域名）删除客户端：

```
spacecmd system_delete FQDN
```

spacecmd system_delete 也删除 Salt key.

system_delete 提供以下选项：

```
usage: system_delete [选项] <系统>
```

选项：

- c TYPE - 可能的值：
- * 'FAIL_ON_CLEANUP_ERR' - 如果发生清理错误则失败，
 - * 'NO_CLEANUP' - 不清理，仅删除，
 - * 'FORCE_DELETE' - 先尝试清理，但在发生错误时仍会删除服务器

6.3. 从命令行删除客户端



This process is for Uyuni clients only. Do not run it on the Uyuni Server itself.



请勿在运行 Red Hat Enterprise Linux、Debian 或克隆的客户端上执行以下过程，而是应使用与 zypper 效果相同的打包器命令，例如 yum、dnf 或 apt。

Procedure: Deleting SLES 12 and 15 Clients

1. 停止 salt-minion 服务：

```
systemctl stop salt-minion
```

2. 去除储存库和配置文件：

```
rm /etc/zypp/repos.d/susemanager\*:channels.repo
rm -r /etc/sysconfig/rhn/
rm -r /etc/salt/
```

3. 去除客户端软件包：

```
zypper rm salt salt-minion python*-salt sle-manager-tools-release
```

过程：Salt 捆绑包客户端 - 手动进行注册清理

1. 要取消注册，请运行以下命令：

```
systemctl stop venv-salt-minion
zypper rm -y venv-salt-minion
rm /etc/zypp/repos.d/susemanager\*:channels.repo /etc/venv-salt-
minion/*
rm -r /etc/venv-salt-minion/*
```

For information about the Salt bundle, see [Client-configuration > Contact-methods-saltbundle](#).

Chapter 7. 客户端操作

In addition to registering, upgrading, installing software, or deleting clients other operations can be performed. Uyuni clients can be managed individually or as a set of clients. A set of clients can grouped with System Set Manager for a one time action or permanently with System Groups.

For advanced client configuratin options general Configuration Management is available. You can obtain Custom System Information, power on or off, and reboot clients using the Uyuni Web UI.

The following sections contain detailed descriptions for each of these operations.

7.1. 软件包管理

客户端使用软件包来安装、卸装和升级软件。



安装或升级软件包时，将自动接受许可证或 EULA。

要管理客户端上的软件包，请导航到----，单击要管理的客户端，然后导航到**系统**，**软件**，**软件包子**选项卡。此部分提供的选项取决于您选择的客户端类型及其当前的通道订阅。

大多数软件包管理操作都可以添加到操作链中。有关操作链的详细信息，请参见 **Reference > Schedule**。

7.1.1. 校验软件包

您可以检查客户端上安装的软件包是否与作为其安装源的数据库的当前状态匹配。系统会对安装的软件包的元数据与数据库中的信息（包括文件校验和、文件大小、权限、拥有者、组和类型）进行比较。

过程：校验安装的软件包

1. 在 Uyuni Web UI 中，导航到----，单击安装了软件包的客户端，然后导航到**系统**，**软件**，**软件包**，**校验子**选项卡。
2. 选择要校验的软件包，然后单击 [校验所选软件包]。
3. 校验完成后，导航到**系统**，**事件**，**历史记录**查看结果。

7.1.2. 比较软件包

您可以将某个客户端上安装的软件包与存储的配置文件进行比较，或者与其他客户端上安装的软件包进行比较。比较时，您可以选择修改选定要匹配的客户端。

将软件包与某个配置文件进行比较之前，您需要先存储一个配置文件。配置文件基于当前安装的客户端上的软件包创建。如果已创建配置文件，您可以使用它安装更多客户端，这些客户端中均会安装相同的软件包。

过程：创建存储的配置文件

1. 在 Uyuni Web UI 中，导航到----，单击配置文件要基于的客户端，然后导航到**系统**，**软件**，**软件包**，**配置文件子**选项卡。

2. 单击 。
3. 键入您的配置文件的名称和说明，然后单击 .

过程：比较客户端软件包

1. 在 Uyuni Web UI 中，导航到 ，单击要比较的客户端，然后导航到 **系统**、**软件**、**安装包**、**配置文件** 选项卡。要与存储的配置文件进行比较，请选择该配置文件，然后单击 。
2. 要与其他客户端进行比较，请选择客户端名称，然后单击  查看两个客户端之间的差别的列表。

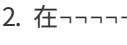
7.2. 补丁管理

您可以在组织中使用自定义补丁来管理客户端。通过这种方式，您可以在自定义通道中发布软件包的补丁警报、安排补丁安装，并在组织中管理补丁。

7.2.1. 创建补丁

要使用自定义补丁，您需要创建一个补丁，向其添加软件包，并将其添加到一个或多个通道。

过程：创建自定义补丁

1. 在 Uyuni Web UI 中，导航到 **补丁**、**管理补丁**，单击 .
2. 在  部分，使用以下细节：
 - 在  字段中，键入补丁的简要说明。
 - 在  字段中，键入补丁的标签。建议您为组织设计一个命名约定，以便于进行补丁管理。
 - 在  字段中，输入补丁的版本号。例如，如果这是该补丁的第一个版本，请使用 1。
 - 在  字段中，选择要使用的补丁类型。例如，针对修复错误的补丁选择 。
 - 如果您选择  建议类型，请在  字段中选择要使用的严重性级别。
 - 在  字段中，键入该补丁所代表的产品的名称。
 - 可选：在  字段中，键入补丁作者的名称。
 - 在  和  字段中填写补丁的其他相关信息。
3. 可选：在 **Bug** 部分，使用以下细节指定任何相关 Bug 的信息：
 - 在  字段中，输入 Bug 编号。
 - 在  字段中，键入 Bug 的简要说明。
 - 在  字段中，键入 Bug 的地址。
 - 在  字段中，键入与该 Bug 有关的任何关键字。请在各关键字之间使用逗号。
 - 在  和  字段中填写 Bug 的其他相关信息。
 - 选择要向其添加新补丁的一个或多个通道。
4. 单击 .

您也可以通过克隆现有补丁来创建补丁。克隆方法会保留软件包关联并简化补丁发布过程。

过程：克隆补丁

1. 在 Uyuni Web UI 中，导航到**补丁**，**克隆补丁**。
2. 在**选择通道**字段中，选择要克隆的补丁对应的软件通道。
3. 选择要克隆的一个或多个补丁，然后单击**[克隆补丁]**。
4. 选择要向其添加克隆的补丁的一个或多个通道。
5. 确认细节以开始克隆。

创建补丁后，您便可以向其指派软件包。

过程：向补丁指派软件包

1. 在 Uyuni Web UI 中，导航到**补丁**，**管理补丁**，然后单击补丁的建议名称以查看补丁细节。
2. 导航到**软件包**，**添加**选项卡。
3. 在**选择通道**字段中，选择包含要指派给补丁的软件包的软件通道，然后单击**[查看软件包]**。您可以选择**[所有通道]**以查看所有通道中的可用软件包。
4. 选择要包含的软件包，然后单击**[添加软件包]**。
5. 确认软件包的细节，然后单击**[确认]**将其指派给补丁。
6. 导航到**软件包**，**列出/去除**选项卡，检查是否已正确指派软件包。

将软件包指派给补丁后，补丁缓存即会更新以反映更改。更新缓存可能需要几分钟时间。

如果您需要更改现有补丁的细节，可以通过**编辑**页面来更改。

过程：编辑和删除现有补丁警报

1. 在 Uyuni Web UI 中，导航到**补丁**，**管理补丁**。
2. 单击补丁的建议名称以查看补丁细节。
3. 根据需要进行更改，然后单击**[更新补丁]**。
4. 要删除补丁，请在**编辑**页面中选择补丁，然后单击**[删除补丁]**。删除补丁可能需要几分钟时间。

7.2.2. 将补丁应用到客户端

某个补丁就绪后，您可以将其单独应用到客户端，也可以与其他补丁一起应用到客户端。

补丁内的每个软件包都来自一个或多个通道。如果客户端未订阅相应通道，将不会安装更新。

如果客户端已安装更新版本的软件包，将不会安装更新。如果客户端安装的是较旧版本的软件包，将会升级该软件包。

过程：应用所有适用的补丁

1. 在 Uyuni Web UI 中，导航到**系统**，**概览**，然后选择要更新的客户端。

2. 导航到软件 › 补丁选项卡。
3. 单击 选择所有适用的补丁。
4. 单击 更新客户端。

如果您是以管理员特权登录的，还可以批量进行更大规模的客户端升级。

过程：将单个补丁应用到多个客户端

1. 在 Uyuni Web UI 中，导航到补丁 › 补丁列表。
2. 找到要应用的补丁，然后单击该补丁对应的----列下面的数字。
3. 选择要应用补丁的客户端，然后单击 。
4. 确认要执行更新的客户端列表。

过程：将多个补丁应用到多个客户端

1. 在 Uyuni Web UI 中，导航到系统 › 概览，然后选中要更新的客户端，以将其添加到系统集管理器。
2. 导航到系统 › 系统集管理器，然后导航到----选项卡。
3. 选择要应用到客户端的补丁，然后单击 .
4. 安排更新的日期和时间，然后单击 .
5. 要查看更新进度，请导航到日程安排 › 待执行的操作。



使用为每个客户端配置的联系方法安装安排的软件包更新。有关详细信息，请参见 [Client-configuration > Contact-methods-intro](#)。

7.3. 系统锁定

系统锁用于防止对客户端执行某些操作。例如，系统锁可防止更新或重启动客户端。此功能对于运行生产软件的客户端或想要阻止意外更改时很有用。您可以在准备好执行操作时禁用系统锁。

7.3.1. System Locks on Clients

When a client is locked, or put into blackout mode, no actions can be scheduled, execution commands are disabled, and a yellow banner is displayed on the System Details page. In this mode, actions can be scheduled for the locked client using the Web UI or the API, but the actions fail.



The locking mechanism is not available for Salt SSH clients.

Procedure: System Locking a Client

1. 在 Uyuni Web UI 中，导航到要锁定的客户端的-----页面。
2. 导航到----选项卡，选中系统锁公式，然后单击 .
3. 导航到公式系统锁选项卡，选中-----，然后单击 。在此页面上，您也可以在客户端处于锁定状态时启用特定的 Salt 模块。

- 进行更改后，您可能需要应用 highstate。在此情况下，Web UI 中会显示一个标题通知您。客户端会保持锁定状态，直到您去除系统锁公式。

For more information about blackout mode in Salt, see <https://docs.saltstack.com/en/latest/topics/blackout/index.html>.

7.3.2. 软件包锁

Package locking can be used on several clients, but different feature sets are available. You must differentiate between SUSE Linux Enterprise and openSUSE (zypp-based) versus Red Hat Enterprise Linux or Debian clients.

7.3.2.1. 基于 Zypp 的系统上的软件包锁

软件包锁用于防止在未经授权的情况下安装或升级软件包。当软件包被锁定后，会显示一个挂锁图标，表示无法安装该软件包。任何尝试安装锁定软件包的操作均会在事件日志中报告为错误。

您无法安装、升级或去除锁定的软件包，无论是通过 Uyuni Web UI 还是使用软件包管理器在客户端计算机上直接执行均是如此。锁定的软件包还会间接锁定任何依赖的软件包。

过程：使用软件包锁

- 在受管系统上导航到软件，软件包，锁定选项卡查看所有可用软件包的列表。
- 选择要锁定的软件包，然[请][求][锁][定]。选择要激活软件包锁的日期和时间。默认情况下，软件包锁会尽快激活。请注意，软件包锁可能不会立即激活。
- 要去除软件包锁，请选择要解锁的软件包，然[请][求][解][锁]。就像激活软件包锁一样选择日期和时间。

7.3.2.2. 类似 Red Hat Enterprise Linux 和 Debian 的系统上的软件包锁



Some Red Hat Enterprise Linux- and Debian-like systems have package locking available on clients.

在类似 Red Hat Enterprise Linux 和 Debian 的系统上，软件包锁仅用于防止在未经授权的情况下升级或去除软件包。当软件包被锁定后，会显示一个挂锁图标，表示无法更改该软件包。任何尝试更改锁定软件包的操作均会在事件日志中报告为错误。

您无法升级或去除锁定的软件包，无论是通过 Uyuni Web UI 还是使用软件包管理器在客户端计算机上直接执行均是如此。锁定的软件包还会间接锁定任何依赖的软件包。

过程：使用软件包锁

- On Red Hat Enterprise Linux 7 systems, install `yum-plugin-versionlock`, and on Red Hat Enterprise Linux 8 or 9 systems, install `python3-dnf-plugin-versionlock` as root. On Debian systems, the `apt` tool has the locking feature included.
- 在受管系统上导航到软件，软件包，锁定选项卡查看所有可用软件包的列表。
- 选择要锁定的软件包，然[请][求][锁][定]。选择要激活软件包锁的日期和时间。默认情况下，软件包

锁会尽快激活。请注意，软件包锁可能不会立即激活。

- 要去除软件包锁，请选择要解锁的软件包，然后 **[请求]**。就像激活软件包锁一样选择日期和时间。

7.4. 配置管理

您可以使用配置文件和通道管理客户端的配置，而无需手动配置每个客户端。

配置参数编写在脚本中并存储在配置文件中。您可以使用 Uyuni Web UI 直接写入配置文件，也可以上载或关联到其他位置存在的文件。

Configuration files can be centrally managed. Centrally managed configuration files are provided by global configuration channels and can be applied to any client subscribed to the Uyuni Server.

配置通道用于组织配置文件。您可以为客户端订阅配置通道，并根据需要部署配置文件。

配置文件有版本控制，因此您可以添加配置设置，在您的客户端上对其进行测试，并根据需要将其回滚到之前的修订版。如果您已创建配置通道，还可以在不同的配置文件以及同一配置文件的不同修订版之间进行比较。

Centrally managed configuration files are provided by global configuration channels.

This table shows the supported features, where:

- ✓ 功能受 SUSE 支持
- ✗ 功能不受 SUSE 支持
- ? 功能正在考虑之中，日后可能受支持，也可能不受支持。

表格 47. 配置管理支持的功能

Feature	Status
Global Configuration Channels	✓
Deploying Files	✓
Comparing Files	?
Locally Managed Files	✓ (with Salt features)
Sandbox Files	✗
Applying the Highstate	✓
File Import from a Client	✗
Jinja Templating	✓
Configuration Macros	✓ (with Salt features: grains, pillar data, etc.)

7.4.1. 创建配置通道

7.4.1.1. Central Configuration Channel

要创建新的中心配置通道，请执行以下操作：

过程：创建中心配置通道

1. 在 Uyuni Web UI 中，导航到配置，通道，然后单击 **[创建配置通道]**。
2. 键入通道的名称。
3. 键入通道的标签。此字段只能包含字母、数字、连字符 (-) 和下划线 (_)。
4. 键入用于与其他通道进行区分的通道说明。
5. 单击 **[创建配置通道]** 以创建新通道。

7.4.1.2. Salt State Channel

You can also use a configuration channel to manage Salt states on clients:

Procedure: Creating a Salt State Channel

1. 在 Uyuni Web UI 中，导航到配置，通道，然后单击 **[创建状态通道]**。
2. 键入通道的名称。
3. 键入通道的标签。此字段只能包含字母、数字、连字符 (-) 和下划线 (_)。
4. 键入用于与其他通道进行区分的通道说明。
5. 为 init.sls 文件键入 SLS 代码。
6. 单击 **[创建配置通道]** 以创建新通道。

7.4.2. 添加配置文件、目录或符号链接

如果您已创建配置通道，则可以添加配置文件、目录或符号链接：

过程：添加配置文件、目录或符号链接

1. 在 Uyuni Web UI 中，导航到配置，通道，单击要向其添加配置文件的配置通道的名称，然后导航到添加文件，创建文件子选项卡。
2. 在 **类型** 字段中，选择是要创建文本文件、目录还是符号链接。
3. 在 **路径** / **目录** 字段中，键入应部署文件的位置的绝对路径。
4. 如果您要创建符号链接，请在 **目标** / **路径** 字段中键入目标文件和路径。
5. 在 **文件** 字段中键入该文件的 **开始** 和 **结束**，以及 **宏**。
6. 如果客户端启用了 SELinux，您可以配置 SELinux **策略** 以启用所需的文件属性（例如用户、角色和文件类型）。
7. 如果配置文件包含宏，请输入标记宏开始位置和结束位置的符号。
8. 在 **文本** 文本框中，使用脚本下拉框选择相应的脚本语言输入配置文件内容。
9. 单击 **[创建文件]**。

7.4.3. 为客户端订阅配置通道

您可以为单个客户端订阅配置通道，方法是导航到**系统**，**系统列表**，选择要使用的客户端，然后导航到——选项卡。要为多个客户端订阅配置通道，可以使用**系统集管理器 (SSM)**。

过程：为多个客户端订阅配置通道

1. 在 Uyuni Web UI 中，导航到**系统**，**系统列表**，然后选择要使用的客户端。
2. 导航到**系统**，**系统集管理器**，然后转到**配置**，**订阅通道**子选项卡，以查看可用配置通道的列表。
3. 可选：单击——列中的数字以查看目前订阅了配置通道的客户端。
4. 选中要订阅的配置通道，然后单击 **[继续]**。
5. 使用向上和向下箭头对配置通道排名。两个配置通道之间的设置发生冲突时，系统会优先使用更靠近列表顶部的通道。
6. 确定通道应用到所选客户端的方式 **[订阅为最低优先]** 将新通道添加为比目前订阅的通道都低的优先级 **[订阅为最高优先]** 将新通道添加为比目前订阅的通道都高的优先级 **[替换现有]** **[有订阅]** 可去除现有通道并将其替换为新通道。
7. 单击 **[应用订阅]**。



如果新配置通道优先级与现有通道冲突，系统会去除重复的通道并根据新优先级进行替换。如果某个操作要对客户端的配置优先级重新排序，Web UI 会要求您在继续之前先确认更改。

7.4.4. 比较配置文件

您也可以使用**系统集管理器 (SSM)** 将客户端上部署的配置文件与存储在 Uyuni 服务器上的配置文件进行比较。

过程：比较配置文件

1. 在 Uyuni Web UI 中，导航到**系统**，**系统列表**，然后选择订阅了要比较的配置文件的客户端。
2. 导航到**系统**，**系统集管理器**，然后转到**配置**，**比较文件**子选项卡，以查看可用配置文件的列表。
3. 可选：单击——列中的数字以查看目前订阅了配置文件的客户端。
4. 选中要比较的配置文件，然后单击 **[安排文件比较]**。

7.4.5. Jinja templating on clients

在 Salt 客户端上可以建立 Jinja 模板。Jinja 通过 pillar 或 grain 提供变量。它们可用于配置文件或 Salt 状态中。

有关详细信息，请参见 <https://docs.saltproject.io/salt/user-guide/en/latest/topics/jinja.html>，该页面包含以下示例：

```

{% if grains.os_family == 'RedHat' %}
  {% set dns_cfg = '/etc/named.conf' %}
{% elif grains.os_family == 'Debian' %}
  {% set dns_cfg = '/etc/bind/named.conf' %}
{% else %}
  {% set dns_cfg = '/etc/named.conf' %}
{% endif %}

dns_conf:
  file.managed:
    - name: {{ dns_cfg }}
    - source: salt://dns/files/named.conf

```

7.5. 电源管理

您可以使用 Uyuni Web UI 打开、关闭和重引导客户端。

此功能使用 IPMI 或 Redfish 协议，通过 Cobbler 配置文件管理。所选客户端的电源管理控制器必须支持以上其中一个协议。

对于 Redfish，请确保您可以在客户端和 Uyuni 服务器之间建立有效的 SSL 连接。您必须信任用于对 Redfish 管理控制器的 SSL 服务器证书签名的证书颁发机构。CA 证书必须为 .pem 格式，并存储在 Uyuni 服务器上的 /etc/pki/trust/anchors/ 中。保存证书后，请运行 update-ca-certificate。

过程：启用电源管理

1. 在 Uyuni Web UI 中，导航到 **系统** > **系统列表**，选择要管理的客户端，然后导航到 **置备** > **电源管理** 选项卡。
2. 在 **协议** 字段中，选择要使用的电源管理协议。
3. 填写电源管理服务器的细节，然后单击要执行的操作的相应按钮，或者单击 **仅保存** 保存细节而不执行任何操作。

您可以将电源管理操作添加到系统集管理器，以将这些操作同时应用到多个客户端。有关使用系统集管理器的详细信息，请参见 **Client-configuration** > **System-set-manager**。

7.5.1. 电源管理和 Cobbler

首次使用电源管理功能时，如果客户端没有相应的 Cobbler 系统记录，将会自动创建该记录。这些自动创建的系统记录无法从网络上引导，其内包含虚设系统映像的引用。之所以需要该引用，是因为 Cobbler 目前不支持没有配置文件或映像的系统记录。

Cobbler 电源管理使用 fence-agent 工具来支持 IPMI 以外的协议。Uyuni 只支持 IPMI 和 Redfish 协议。您可以将客户端配置为使用其他协议，方法是以逗号分隔列表形式将 fence- agent 名称添加到 rhn.conf 配置文件中的 java.power_management.types 配置参数。

7.6. 自定义系统信息

You can include customized system information about your clients. System information is defined as key:value pairs, which can be assigned to clients. For example, you can define a key:value pair for a particular processor, then assign that key to all clients that have that processor installed. Custom system information is categorized, and can be searched using the Uyuni Web UI.

开始前，需要创建可让您存储自定义信息的键。

过程：创建自定义系统信息键

1. 在 Uyuni Web UI 中，导航到 **系统 > 自定义系统信息**，然后单击 **[新建]**。
2. 在 **键** 字段中，添加键的名称。不要使用空格。例如，intel-x86_64-quadcore。
3. 在 **值** 字段中，提供任何其他所需信息。
4. 对需要创建的每个键重复以上步骤。

The information is available via Salt pillar. You can retrieve this information with a command such as:

```
salt $minionid pillar.get custom_info:key1
```

此命令将产生类似如下的输出：

```
$minionid:
  val1
```

创建了一些自定义系统信息键之后，您便可以将其应用到客户端。

过程：将自定义信息键应用到客户端

1. 在 Uyuni Web UI 中，导航到 **客户端**，单击要应用自定义信息的客户端，然后导航到 **细节 > 自定义信息** 选项卡。
2. 单击 **[新建]**。
3. 找到要应用的值，然后单击键标签。
4. 在 **值** 字段中，提供任何其他信息。
5. 单击 **[更新]** 以向客户端应用自定义信息。

有关配置管理的详细信息，请参见 **Client-configuration > Configuration-management**。

7.7. 系统集管理器

系统集管理器 (SSM) 可用于同时对多个客户端执行操作。SSM 会创建多组临时客户端，将它们变为可用状态，以执行您需要应用到多个客户端的一次性操作。如果您需要存留时间更长的客户端组，请考虑使用系统组。有关系统组的详细信息，请参见 **Client-configuration > System-groups**。

下表列出了可在 SSM 中使用的操作。此表中图标的含意如下：

- ✓ 在 SSM 中，此操作可用于此客户端类型
- ✗ 在 SSM 中，此操作不可用于此客户端类型
- ? 正在考虑将此操作用于此客户端类型，日后可能支持此操作，也可能不支持此操作。

表格 48. 可用的 SSM 操作

List systems	✓
Install patches	✓
Schedule patch updates	✓
Upgrade packages	✓
Install packages	✓
Remove packages	✓
Verify packages	✗
Create groups	✓
Manage groups	✓
Channel memberships	✓
Channel subscriptions	✗
Deploy/diff channels	✗
Autoinstall clients	✗
Tag for snapshot	✗
Remote commands	✗
Power management	✗
Update system preferences	✓
Update hardware profiles	✓
Update package profiles	✓
Set/remove custom values	✓
Reboot clients	✓
Migrate clients to another organization	✓
Delete clients	✓

您可以通过多种方式选择 SSM 的客户端：

- 导航到**系统** > **系统列表**，然后选中要使用的客户端。
- 导航到**系统** > **系统组**，然后针对要使用的系统组单击[在 SSM 中 使用]。
- 导航到**系统** > **系统组**，选中要使用的组，然后单击[使用组]。

选择要使用的客户端后，导航到**系统 > 系统集管理器**，或单击顶部菜单栏中的`-----`图标。



SSM 中的细节与 Uyuni Web UI 其他部分中的细节略有不同。在 SSM 中，所有可用的更新都会显示。这样您可以升级到可能不是最新版本的软件包。

7.7.1. 在 SSM 中更改基础通道

您可以使用 SSM 同时更改多个客户端的基础通道。



更改基础通道会大量更改可用于受影响客户端的软件包和补丁。须谨慎使用该功能。

过程：使用 SSM 更改多个客户端的基础通道

1. 在 Uyuni Web UI 中，导航到**系统 > 系统列表**，选中要使用的客户端，然后导航到**系统 > 系统集管理器**。
2. 导航到`-----`子选项卡。
3. 在列表中找到当前的基础通道，并校验`-----`列中显示的数字是否正确。您可以单击此列中的数字查看要更改的客户端的更多细节。
4. 在`-----`字段中选择新基础通道，然后单击`[下一步]`。
5. 对于每个子通道，选择`-----`、`-----`或`-----`，然后单击`[下一步]`。
6. 选中要进行的更改，然后选择希望操作执行的时间。
7. 单击`[确定]`安排更改。

7.8. 系统组

通过系统组，您可以更轻松地管理大量客户端。组可用于对客户端执行批量操作，例如应用更新、配置通道、Salt 状态或公式。

您可以采用任何适合环境的方式来对客户端分组。例如，可以按客户端上安装的操作系统、所在的实际位置或所处理的工作负载类型来组织客户端。客户端可以划分到任意数量的组中，因此您可以采用不同的方式来定义组。

When you have clients organized into groups, you can perform updates on all clients in one or more groups, or on intersections between groups. For example, you can define one group for all clients with web server software, and another group for all SLES clients. You can then perform updates on all clients with web server software, or use the intersection between the groups, and update all SLES clients with web server software.

7.8.1. 创建组

在使用组对客户端分组之前，需要先创建一些组。

过程：创建新系统组

1. 在 Uyuni Web UI 中，导航到**系统 > 系统组**。

2. 单击 。
3. 指定新组的名称和说明。
4. 单击  以保存组。
5. 对需要创建的每个组重复以上步骤。

7.8.2. 将客户端添加到组

您可以向组中添加单个客户端，也可以同时添加多个客户端。

过程：将单个客户端添加到组

1. 在 Uyuni Web UI 中，导航到 **系统**，**系统列表**，然后单击要添加的客户端的名称。
2. 导航到 **组**，**加入** 选项卡。
3. 选中要加入的组，然后单击 。

过程：将多个客户端添加到组

1. 在 Uyuni Web UI 中，导航到 **系统**，**系统列表**，然后单击要向其添加客户端的组的名称。
2. 导航到 **添加系统** 选项卡。
3. 选中要添加的客户端，然后单击 .

过程：使用 SSM 将多个客户端添加到组

1. 在 Uyuni Web UI 中，导航到 **系统**，**系统列表**，然后选中要添加的每个客户端，这会将这些客户端添加到系统集管理器中。
2. 导航到 **系统**，**系统集管理器**，然后转到 **→** 选项卡。
3. 找到要加入的组并选中 .
4. 单击 .
5. 单击  将客户端加入所选的组。

有关系统集管理器的详细信息，请参见 [Client-configuration > System-set-manager](#)。

You can see which clients are in a group by navigating to **Systems** > **System Groups**, clicking the name of the group, and navigating to the **Systems** tab.

7.8.3. 使用组

When you have your clients arranged into groups, you can use your groups to manage updates.

在 Uyuni Web UI 中，导航到 **系统**，**系统组**。如果组中的任何客户端有可用更新，列表会显示相应图标。如果组中有任何客户端的检查更新状态功能被禁用，列表会显示问号。单击图标可查看有关可用更新的详细信息，并向客户端应用更新。

您也可以同时使用多个组。选择要使用的多个组，然后单击  以选择每个选定组中的每个客户端。

Alternatively, you can work on intersections of groups. Select two or more groups, and click **[Work with intersection]** to select only those clients that exist in all the selected groups. For example, you might have one group for all clients with web server software, and another group for all SLES clients. The intersection of these groups would be all SLES clients with web server software.

7.9. 系统类型

客户端按系统类型分类。每个客户端都可以被指派一个基础系统类型和一个附加系统类型。

Base system type is Salt for all clients.

附加系统类型包括———（作为虚拟主机运行的客户端）和———（作为构建主机运行的客户端）。

您可以导航到系统 > 系统列表 > 系统类型调整附加系统类型。选中要更改其附加系统类型的客户端，选择———，然后单击———或———。

Chapter 8. 操作系统安装

通常，您注册的是已经在运行的客户端。您可能是在将这些计算机注册到 Uyuni 之前手动安装了它们，也可能它们是在您将 Uyuni 添加到您的环境之前就已安装的现有系统。

您也可以使用 Uyuni 一次性完成安装操作系统和将其注册到 Uyuni 的操作。此方法部分或完全自动化，因此可为您节省回答安装程序问题的时间，特别适合您有许多客户端需要安装和注册的情况。

可通过多种方法从 Uyuni 安装操作系统：

- 在已注册的客户端上就地安装；
- 使用 PXE 引导通过网络安装；
- 准备安装 CD-ROM 或 USB 密钥，然后转到计算机在该媒体上进行引导；
- 作为 Uyuni for Retail 解决方案的一部分安装。

就地安装方法假设客户端上已经安装了以前的操作系统，并且客户端已注册到 Uyuni。

有关就地安装方法的信息，请参见 **Client-configuration > Autoinst-reinstall**。

网络引导安装方法适用于未格式化的计算机。不过，该方法只能在特定网络配置中执行：

- Uyuni 服务器（或其代理之一）与您要安装的计算机位于同一本地网络中，或者您具有可用于跨越两者之间的所有路由器的 DHCP 中继；
- 您能够设置新的 DHCP 服务器或配置现有的 DHCP 服务器；
- 要安装的客户端能够使用 PXE 引导，并且您可以如此配置它们。

可移动媒体方法可让您绕过这些网络约束。但是，该方法假设计算机能够读取 CD-ROM 或 USB 密钥，并从它们引导。它还需要对客户端计算机进行物理访问。

有关可移动媒体方法的信息，请参见 **Client-configuration > Autoinst-cdrom**。

有关 Uyuni for Retail 方法的信息，请参见 **Retail > Retail-overview**。



不支持自动安装 Ubuntu 和 Debian 客户端。必须手动安装这些操作系统。

Uyuni 的自动安装功能基于名为 Cobbler 的软件运行。有关 Cobbler 的详细信息，请访问 <https://cobbler.readthedocs.io>。



SUSE 仅支持 Uyuni Web UI 中或通过 Uyuni API 提供的 Cobbler 功能。Cobbler 支持的唯一一个命令行命令为 buildiso。本文中所述的仅为支持的功能。

8.1. 重新安装已注册系统

就地重新安装从本地客户端系统开始。因此，客户端不需要具有使用 PXE 通过网络引导的能力。

要就地重新安装已注册客户端，必须定义可自动安装的发行套件和自动安装配置文件。有关信息，请参见 [Client-configuration > Autoinst-distributions](#) 和 [Client-configuration > Autoinst-profiles](#)。

定义自动安装配置文件和发行套件后，便可执行重新安装。

过程：重新安装已注册客户端

1. 在 Uyuni Web UI 中，导航到 **系统**，**系统列表**，选择要重新安装的客户端，然后转到 **置备**，**自动重新安装**，**日程安排** 选项卡。
2. 选择您准备的自动安装配置文件，根据需要选择代理，然后单击 **[日程安排] [自动安装] [完成]**。
3. 您可以导航到 **置备**，**自动安装**，**会话状态** 来监视安装进度，也可以直接在客户端上监视。客户端将重引导，并在引导菜单中选择名为 `reinstall-system` 的新选项。

安装随即会通过 HTTP 协议进行。

8.2. 通过 CD-ROM 或 USB 密钥安装

对于尚未注册到 Uyuni 的客户端，如果无法通过 PXE 进行网络引导，可以使用可引导 CD-ROM 或 USB 密钥来安装系统。

准备此类可移动媒体的其中一个方法是使用 Cobbler。有关使用 Cobbler 准备 ISO 映像的信息，请参见[使用 Cobbler 构建 ISO 映像](#)。

对于 SUSE 系统，通常建议使用 KIWI 来准备 ISO 映像。有关详细信息，请参见[使用 KIWI 构建 SUSE ISO 映像](#)。

在所有情况下，您都需要使用生成的映像刻录 CD-ROM 或准备 USB 密钥。

8.2.1. 使用 Cobbler 构建 ISO 映像

Cobbler 可创建包含一组发行套件、内核和菜单的 ISO 引导映像。该映像的工作方式与 PXE 安装类似。



IBM Z 上不支持使用 Cobbler 构建 ISO。

与通过 PXE 进行网络引导类似，为了使用 Cobbler 准备 ISO 映像，您需要准备发行套件和配置文件。有关创建发行套件的信息，请参见 [Client-configuration > Autoinst-distributions](#)。有关创建配置文件的信息，请参见 [Client-configuration > Autoinst-profiles](#)。

The Cobbler `buildiso` command takes parameters to define the name and output location of the boot ISO. Specifying the distribution with `--distro` is mandatory when running `buildiso` command.

```
cobbler buildiso --iso=/path/to/boot.iso --distro=<发行套件标签>
```



必须按 Cobbler 中所列的名称（而不是简单地按 UI 中所示）使用发行套件和配置文件标签。

要列出 Cobbler 存储的发行套件和配置文件的名称，请运行以下命令：

```
# cobbler distro list
# cobbler profile list
```

引导 ISO 默认包含所有配置文件和系统。您可以通过 `--profiles` 和 `--systems` 选项来限制使用的配置文件和系统。例如：

```
cobbler buildiso --systems="系统 1 系统 2 系统 3" \
--profiles=<配置文件 1 标签> <配置文件 2 标签> <配置文件 3 标签> --
distro=<发行套件标签>
```



如果您无法将 ISO 映像写入到公共 tmp 目录,请检查 /usr/lib/systemd/system/cobblerd.service 中的 systemd 设置。

8.2.2. 使用 KIWI 构建 SUSE ISO 映像

KIWI 是一个映像创建系统。您可以使用 KIWI 创建供目标系统用于安装 SUSE 系统的可引导 ISO 映像。重引导或打开系统时，它会从映像引导，从 Uyuni 装载 AutoYaST 配置，并根据 AutoYaST 配置文件安装 SUSE Linux Enterprise Server。

要使用 ISO 映像，请引导系统并在提示符处键入 `autoyast`（假设您将 AutoYaST 引导的标签保留为 `autoyast`）。按 `kbd: [Enter]` 开始 AutoYaST 安装。

有关 KIWI 的详细信息，请参见 <http://doc.opensuse.org/projects/kiwi/doc/>。

8.2.3. 使用 Cobbler 构建 Red Hat ISO 映像

有关详细信息，请参见 [client-configuration:autoinst-cdrom.pdf](#)。

8.3. 可自动安装的发行套件

自动安装过程依赖于几个文件来启动安装。这些文件包括 Linux 内核、初始 RAM 磁盘和在安装模式下引导操作系统所需的其他文件。

Uyuni uses the `mgradm` tool to copy the installation file from the source to the server container.

您可以从 DVD 映像中提取所需的文件。有关信息，请参见 [基于 ISO 映像的发行套件](#)。

或者，您也可以安装 `tftpboot-installation` 软件包。有关信息，请参见 [基于 RPM 软件包的发行套件](#)。

对于与这些文件相同的操作系统版本，您还必须在 Uyuni 服务器上同步基础通道。

当您准备好文件并已同步基础通道时，您需要声明发行套件。此操作会将安装文件关联到基础通道。发行套件

可能会由一个或多个安装配置文件引用。有关信息，请参见[声明可自动安装的发行套件](#)。

8.3.1. 基于 ISO 映像的发行套件

此方法假设您有要在客户端上安装的操作系统的安装媒体。这通常是 DVD .iso 映像，其中包含 Linux 内核、initrd 文件和在安装模式下引导操作系统所需的其他文件。

过程：从安装媒体导入文件

1. Use `mgradm` to import installation data from the ISO image:

```
# mgradm distribution copy <image_name>.iso <image_name>
```

2. Take a note of the distribution path reported by `mgradm`. You will need it when you declare the distribution to Uyuni.

8.3.1.1. Distribution autodetection and registration

`mgradm` is able to automatically detect distribution name and register it to the server. Provided ISO image needs to contain a `.treeinfo` file.

Procedure: Import distribution file with autodetection and registration

1. Use `mgradm`:

```
# mgradm distribution copy --api-user <username> --api-password <password> <image_name>.iso
```

8.3.2. 基于 RPM 软件包的发行套件

此方法适用于 SUSE 系统。它比从安装媒体导入内容更简单，因为它使用的是安装系统的预打包文件。

过程：从安装软件包提取文件

1. 在 Uyuni 服务器上，安装名称以 `tftpboot-installation` 开头的软件包。您可以通过 `zypper se tftpboot-installation` 命令确定它的确切名称
2. You can install the package to different root to avoid need for restart using following command:

```
# mkdir /opt/tftpinstall
# zypper --installroot /opt/tftpinstall install tftpboot-
installation-SLE-Micro-5.5-x86_64
```

3. Find the installation files with the command `ls -d /opt/tftpinstall/usr/share/tftpboot-installation/*.`

4. Copy installation files using `mgradm`:

```
# mgradm distribution copy /opt/tftpinstall/usr/share/tftpboot-
installation/SLE-Micro-5.5-x86_64 SLE-Micro-5.5-x86_64
```

5. Take a note of the distribution path reported by `mgradm` tool. You will need it when you declare the distribution to Uyuni.

6. After `mgradm` tool finishes, you can remove `/opt/tftpinstall` directory.

此过程将准备安装与驱动 Uyuni 服务器的操作系统版本相同的操作系统版本。如果您想在客户端上安装不同的操作系统或版本，需要从其所属的发行套件手动获取 `tftpboot-installation-*` 软件包。在 Uyuni 的-----输入框中，搜索名称以 `tftpboot-installation` 开头的软件包，然后查看软件包的细节。`/var/spacewalk/` 下会显示本地路径。

8.3.3. 声明可自动安装的发行套件

提取自动安装文件后，接下来要声明可自动安装的发行套件。

过程：声明可自动安装的发行套件

1. 在 Uyuni Web UI 中，导航到 **系统** > **自动安装** > **发行套件**。

2. 单击-----，并填写以下字段：

- 在-----字段中，输入用于识别可自动安装的发行套件的名称。
- 在-----字段中，输入保存在 Uyuni 服务器上的安装媒体的路径。
- 选择匹配的-----。所选值必须与安装媒体相匹配。
- 选择-----。所选值必须与安装媒体相匹配。
- 可选：指定引导此发行套件时要使用的内核选项。您可以通过多种方式来提供内核选项。此处仅添加了发行套件通用的选项。

3. 单击 **[创建可自动安装的发行套件]**。

您准备的安装文件可能不包含需要安装的软件包。如果这些软件包未包含在内，请将 `useonlinerepo=1` 添加到-----字段。

软件包储存库包含的元数据有可能未签名。如果元数据未签名，请将 `insecure=1` 添加到-----字段，或者使用您自己的 GPG 密钥（如 **Client-configuration** > **Autoinst-ownpgpkey** 中所述）。

有些情况下需要这些内核选项，例如，当您使用“联机安装程序”ISO 映像而非完整的 DVD 时，或者当您使用 `tftpboot-installation` 软件包时。

导航到 **系统** > **自动安装** > **发行套件** 可管理您的可自动安装的发行套件。

8.4. 自动安装配置文件

自动安装配置文件决定了如何安装操作系统。例如，您可以指定更多要传递给安装程序的内核参数。

配置文件最重要的部分是“自动安装文件”。手动执行安装时，必须向安装程序提供相关信息，例如分区和网络信息以及用户细节。您可以使用自动安装文件以脚本形式提供此类信息。这种类型的文件有时也称为“答案文件”。

在 Uyuni 中，您可以使用两种不同的配置文件，具体取决于您要安装的客户端的操作系统：

- 对于 SUSE Linux Enterprise 或 openSUSE 客户端，请使用 AutoYaST。
- 对于 Red Hat Enterprise Linux 客户端，请使用 Kickstart。

如果您要安装具有不同操作系统的客户端，可以使用 AutoYaST 和 Kickstart 配置文件。

- 有关如何声明配置文件的信息，请参见[声明配置文件](#)。
- 有关 AutoYaST 配置文件的信息，请参见[AutoYaST 配置文件](#)。
- 有关 Kickstart 配置文件的信息，请参见[Kickstart 配置文件](#)。

配置文件中包含的自动安装文件可以包含变量和代码段。有关变量和代码段的信息，请参见[模板语法](#)。

8.4.1. 声明配置文件

准备好自动安装文件和发行套件后，您可以创建配置文件来管理 Uyuni 服务器上的自动安装。配置文件会决定如何安装您选择的此发行套件。创建配置文件的其中一个方式是上载 AutoYaST 或 Kickstart 文件。或者，您也可以使用 Web UI 向导（仅针对 Kickstart）。

过程：通过上载创建自动安装配置文件

1. 在 Uyuni Web UI 中，导航到系统，自动安装，配置文件。
2. 单击 上载 Kickstart/AutoYaST 文件。
3. 在名称字段中，键入配置文件的名称。不要使用空格。
4. 在发行套件字段中，选择要用于此配置文件的可自动安装的发行套件。
5. 在虚拟化类型字段中，选择要用于此配置文件的虚拟化类型，或选择--（如果您不想使用此配置文件创建新的虚拟机）。
6. 将自动安装文件的内容复制到内容字段，或使用直接上载文件。

有关此处要包含的细节的详细信息，请参见[AutoYaST 配置文件](#)或[Kickstart 配置文件](#)。

7. 单击 创建 以创建配置文件。

过程：通过向导创建 Kickstart 配置文件

1. 在 Uyuni Web UI 中，导航到系统，自动安装，配置文件。
2. 单击 创建 Kickstart 配置文件。

3. 在 **配置文件名称** 字段中，键入配置文件的名称。不要使用空格。
4. 在 **基础通道** 字段中，选择要用于此配置文件的基础通道。系统会根据可用的发行套件填充此字段。如果您需要的基础通道不可用，请检查您是否正确创建了发行套件。
5. 在 **虚拟化类型** 字段中，选择要用于此配置文件的虚拟化类型，或选择 **不进行虚拟化**。
6. 单击 **[下一步]**。
7. 在 **安装媒体路径** 中，键入 Uyuni 服务器上安装的安装媒体的路径。
8. 单击 **[下一步]**。
9. 提供客户端上 root 用户的口令。
10. 单击 **[完成]**。
11. 查看新配置文件的细节，并视需要进行自定义。

创建自动安装配置文件时，您可以选中 **从发行套件自动提取配置文件**。此设置可让 Uyuni 自动提取与指定基础通道关联的最新发行套件。如果您以后添加新发行套件，Uyuni 会使用最近创建或修改的发行套件。

更改 **发行套件** 通常需要更改配置文件加载程序和分区选项。这会重写您的自定义设置。请在保存前导航到 **发行套件** 选项卡校验新的或更改后的设置。

来自发行套件和配置文件的内核选项会进行合并。

您可以更改自动安装配置文件的细节和设置，方法是导航到 **系统 > 自动安装 > 配置文件**，然后单击要编辑的配置文件的名称。或者，可导航到 **系统 > 系统列表**，选择要置备的客户端，然后导航到 **置备 > 自动安装子选项卡**。

8.4.2. AutoYaST 配置文件

AutoYaST 配置文件由标识该配置文件的 **名称**、指向可自动安装的发行套件的 **发行套件**、各种选项以及最重要的 AutoYaST 安装文件组成。

AutoYaST 安装文件是一个 XML 文件，用于向 AutoYaST 安装程序提供指示。AutoYaST 将其称为“控制文件”。有关 AutoYaST 安装文件的完整语法，请参见 <https://doc.opensuse.org/projects/autoyast/#change-configuration-installation-options>。

SUSE 提供了 AutoYaST 安装文件模板，您可以基于它们创建自己的自定义文件。您可在 <https://github.com/SUSE/manager-build-profiles> 上的 AutoYast 目录中找到这些模板。使用前，需要为其中的每个配置文件设置一些变量。请参见脚本随附的 README 文件确定您需要的变量。有关在 AutoYaST 脚本中使用变量的详细信息，请参见 [变量](#)。

在 AutoYaST 安装文件中，用于通过 Uyuni 安装的最重要的部分如下：

- `<add-on>` 允许添加子通道到安装。例如，参见 <https://doc.opensuse.org/projects/autoyast/#Software-Selections-additional>。
- `<general>$SNIPPET('spacewalk/sles_no_signature_checks')</general>` 禁用签名检查
- `<software>` 用于为 Unified Installer 指定产品

- See <https://doc.opensuse.org/projects/autoyast/#CreateProfile-Software> with a "<software>" example
- <init-scripts config:type="list">\$SNIPPET('spacewalk/minion_script')</init-scripts> 用于将客户端作为 Salt 客户端注册到 Uyuni。

有关 AutoYaST 的详细信息，请参见 <https://doc.opensuse.org/projects/autoyast/>。

A more recent, Salt-based alternative to AutoYaST, is Yomi. For information about Yomi, see [Specialized-guides > Salt](#).

8.4.3. Kickstart Profiles

Kickstart 配置文件提供了大量配置选项。要创建这些配置文件，您可以上载它们，也可以使用专用向导。

Kickstart 配置文件允许您使用文件保留列表。如果您有许多自定义配置文件位于要使用 Kickstart 重新安装的客户端上，则可以将它们保存为列表，并将该列表与 Kickstart 配置文件相关联。

Procedure: Creating a File Preservation List

- 在 Uyuni Web UI 中，导航到系统，自动安装，文件保留，然后单击 **[创建文件保留列表]**。
- 输入适当的标签，并列出要保存的所有文件和目录的绝对路径。
- 单击 **[创建列表]**。
- 将该文件保留列表包含到 Kickstart 配置文件中。
- 导航到系统，自动安装，配置文件，选择要编辑的配置文件，转到系统细节，文件保留子选项卡，然后选择要包含的文件保留列表。



文件保留列表总大小上限为 1 MB。`/dev/hda1` 和 `/dev/sda1` 等特殊设备无法保留。只能使用文件名和目录名，不能使用正则表达式通配符。

有关 Kickstart 的详细信息，请参见 Red Hat 文档。

8.4.4. Templates Syntax

安装文件的部分内容在安装过程中会被替换。变量会被替换为相应的单个值，代码段会被替换为整段文本。转义符或转义部分不会被替换。

名为 Cheetah 的模板引擎允许 Cobbler 进行这些替换。利用此机制，您在重新安装大量系统时就无需为每个系统手动创建配置文件。

您可以在 Uyuni Web UI 中创建自动安装变量和代码段。在配置文件中，`-----` 选项卡可让您查看替换的结果。

- 有关变量的信息，请参见 [变量](#)。
- 有关代码段的信息，请参见 [代码段](#)。
- 有关转义符或文本块的信息，请参见 [转义](#)。

8.4.4.1. 变量

可以使用自动安装变量来替换 Kickstart 和 AutoYaST 配置文件中的值。要定义变量，请从配置文件中导航到子选项卡，然后在文本框中创建 name=value 对。

例如，您可以创建一个变量来存储客户端的 IP 地址，创建另一个变量来存储其网关的地址。然后可以为通过同一配置文件安装的所有客户端定义这些变量。要执行此操作，请将下面几行添加到文本框中：

```
ipaddr=192.168.0.28
gateway=192.168.0.1
```

要使用变量，请在配置文件中附加一个 \$ 符号来替换相应值。例如，Kickstart 文件的 network 部分可能如下所示：

```
network --bootproto=static --device=eth0 --onboot=on --ip=$ipaddr \
--gateway=$gateway
```

\$ipaddr 会解析为 192.168.0.28，\$gateway 会解析为 192.168.0.1。

在安装文件中，变量使用层次结构。系统变量优先于配置文件变量，而配置文件变量优先于发行套件变量。

8.4.4.2. Code Snippets

Uyuni 附带了大量预定义的代码段。导航到 **系统** > **自动安装** > **自动安装代码段**，以查看现有代码段列表。

通过在自动安装文件中插入 \$SNIPPET() 宏来使用代码段。例如，在 Kickstart 中，插入该宏：

```
$SNIPPET('spacewalk/rhel_register_script')
```

或者，在 AutoYaST 中，插入该宏：

```
<init-scripts config:type="list">
  $SNIPPET('spacewalk/sles_register_script')
</init-scripts>
```

宏会经过 Cobbler 的分析，并会替换为代码段的内容。您还可以存储自己的代码段，以供日后在自动安装文件中使用。单击 **创建代码段** 以创建新代码段。

下面的示例设置了通用硬盘分区配置的 Kickstart 代码段：

```

clearpart --all
part /boot --fstype ext3 --size=150 --asprimary
part / --fstype ext3 --size=40000 --asprimary
part swap --recommended

part pv.00 --size=1 --grow

volgroup vg00 pv.00
logvol /var --name=var vgname=vg00 --fstype ext3 --size=5000

```

下面是使用该代码段的一个示例：

```
$SNIPPET('my_partition')
```

8.4.4.3. 转义

如果自动安装文件包含 `$example` 这样的外壳脚本变量，则需要使用反斜杠对内容进行转义：`\$(example)`。对 `$` 符号进行转义可防止模板引擎将该符号评估为内部变量。

可以使用 `\#raw` 和 `\#end raw` 指令封装代码段或脚本等文本块，从而对其进行转义。例如：

```

#raw
#!/bin/bash
for i in {0..2}; do
    echo "$i - Hello World!"
done
#end raw

```

所有包含 `#` 符号后接空格的行均视为注释行，因此不会对其进行评估。例如：

```

# start some section (此为注释)
echo "Hello, world"
# end some section (此为注释)

```

8.5. 无人照管的置备

您可以使用 API 调用来声明通过 MAC 地址标识的客户端与自动安装配置文件之间的关联。系统下次重引导时，会根据指定的配置文件开始安装。

过程：通过手动声明的配置文件重新安装

1. 在 Uyuni 服务器上的命令提示符处，使用 `system.createSystemRecord` API 调用。在此示例中，请

将 `name` 替换为您的客户端名称，将 `<profile>` 替换为配置文件标签，将 `<iface>` 替换为客户端上的接口名称（例如 `eth0`），将 `<hw_addr>` 替换为其硬件地址（例如 `00:25:22:71:e7:c6`）：

```
$ spacecmd api -- --args '[ "<name>" , "<profile>" , "" , "" , \
[ { "name": "<iface>" , "mac": "<hw_addr>" } ] ]' \
system.createSystemRecord
```

2. 打开客户端。它会从网络进行引导，并且系统会选择正确的配置文件以执行安装。

此命令会在 Cobbler 中创建一个系统记录。您也可以指定其他参数，例如内核选项、客户端的 IP 地址及其域名。有关详细信息，请参见 `createSystemRecord` 的 API 文档。

8.6. 使用您自己的 GPG 密钥

如果用于自动安装的储存库包含未签名的元数据，则您通常必须使用 `insecure=1` 内核参数作为可自动安装的发行套件的选项，并在 AutoYaST 安装文件中使用 `spacewalk/sles_no_signature_checks` 代码段。

更为安全的替代方案是提供您自己的 GPG 密钥。



此方法仅适用于 SUSE 客户端。

Procedure: Include Your Own GPG Key

1. 创建 GPG 密钥。
2. 使用它对软件包的元数据签名。
3. 将其添加到安装媒体的初始 RAM 磁盘中。
 - 有关如何创建密钥并使用它对元数据签名的信息，请参见 [Administration > Repo-metadata](#)。
 - 有关如何将密钥添加到用于网络引导的安装媒体的信息，请参见 [用于 PXE 引导的自己的 GPG 密钥](#)。
 - 有关如何将密钥添加到用于从 CD-ROM 引导的安装媒体的信息，请参见 [CD-ROM 中的自己的 GPG 密钥](#)。



在您使用新 GPG 密钥对元数据签名时，任何已进行初始配置的客户端都不会知道这个新密钥。理想情况下，您应当在注册任何客户端之前对元数据签名。

如果一些已初始配置的客户端使用的是这些储存库，可以暂时对它们禁用 GPG 密钥检查。

8.6.1. 用于 PXE 引导的自己的 GPG 密钥

PXE 引导过程使用的初始 RAM 磁盘 (`initrd`) 通常只包含 SUSE 的 GPG 密钥。您必须将自己的密钥添加到此文件中，这样就能使用它来检查软件包。



To access a shell inside the Server container run `mgrctl term` on the container host.

过程：将 GPG 密钥添加到初始 RAM 磁盘中

1. 创建一个目录，其路径与引导过程中用来查找 GPG 密钥的路径相同：

```
mkdir -p tftpboot/usr/lib/rpm/gnupg/keys
```

2. 将您的 GPG 密钥复制到此目录中，并加上 .asc 后缀：

```
cp /srv/www/htdocs/pub/mgr-gpg-pub.key
tftpboot/usr/lib/rpm/gnupg/keys/mgr-gpg-pub.asc
```

3. 在顶层目录中，将内容打包并附加到属于安装媒体文件一部分的 `initrd` 中：

```
cd tftpboot
find . | cpio -o -H newc | xz --check=crc32 -c >> /path/to/initrd
```

8.6.2. Own GPG Key in a CD-ROM

您可以使用 `mksusecd` 实用程序修改安装映像。此实用程序包含在开发工具模块中。

过程：将 GPG 密钥添加到安装 ISO 映像中

1. 创建一个目录，其路径与引导过程中用来查找 GPG 密钥的路径相同：

```
mkdir -p initrdroot/usr/lib/rpm/gnupg/keys
```

2. 将您的 GPG 密钥复制到此目录中，并加上 .asc 后缀：

```
cp /srv/www/htdocs/pub/mgr-gpg-pub.key
initrdroot/usr/lib/rpm/gnupg/keys/mgr-gpg-pub.asc
```

3. 使用 `mksusecd` 修改现有的 ISO 映像：

```
mksusecd --create <new-image>.iso --initrd initrdroot/ <old-image>.iso
```

Chapter 9. 虚拟化

You can use Uyuni to manage virtualized clients. In this type of installation, a virtual host is installed on the Uyuni Server to manage any number of virtual guests. If you choose to, you can install several virtual hosts to manage groups of guests.

虚拟化客户端具有的功能范围取决于您选择的第三方虚拟化提供者。

您可以直接在 Uyuni 中管理 Xen 和 KVM 主机及 Guest。采用这种方式，您可以使用 AutoYaST 或 Kickstart 自动安装主机和 Guest，并在 Web UI 中管理 Guest。

对于 VMWare（包括 VMWare vSphere）和 Nutanix AHV，Uyuni 需要您设置虚拟主机管理器（VHM）来控制 VM。这样您便能控制主机和 Guest，但与使用 Xen 和 KVM 相比，受到的限制会更多。Uyuni 无法在 VMWare vSphere 或 Nutanix AHV 上创建和编辑 VM。

Uyuni 不直接支持其他第三方虚拟化提供者。不过，如果您的提供者允许您导出 VM 的 JSON 配置文件，您可以将该配置文件上载到 Uyuni 并使用 VHM 进行管理。

有关使用 VHM 来管理虚拟化的详细信息，请参见 [Client-configuration > Vhm](#)。

9.1. Manage Virtualized Hosts

Before you begin, ensure that the client you want to use as a virtualization host has the Virtualization Host system type assigned to it. Navigate to **Systems > Systems List** and click the name of the client to use as a virtualization host. If the Virtualization Host system type is not listed, initialize the virtualization Host formula. For more information, see [client-configuration:virt-xenkvm.pdf](#).

客户端具有“Virtualization Host”系统类型后，该客户端的“系统细节”页面中便会显示“Virtualization Host”选项卡。“Virtualization Host”选项卡可用于创建和管理虚拟 Guest，以及管理存储池和虚拟网络。

9.2. 创建虚拟 Guest

您可以在 Uyuni Web UI 中向虚拟化主机添加虚拟 Guest。

过程：创建虚拟 Guest

1. 在 Uyuni Web UI 中，导航到 **系统 > 系统列表**，单击虚拟化主机的名称，然后导航到“Virtualization Host”选项卡。

2. 在“Guest”部分，填写以下细节：

- 在 Guest 子选项卡中，单击 [Create Guest]。
- 在“Name”字段中，键入 Guest 的名称。
- 在“Management”字段中，选择要使用的超级管理程序。
- 在“Type”字段中，选择全虚拟化或半虚拟化。
- 在“Memory”字段中，以 MiB 为单位键入 Guest 磁盘的大小上限。
- 在“vCPU”中，键入 Guest 的 vCPU 数量。

- 在“CPU”字段中，选择要在 Guest 上使用的模拟 CPU 体系结构。默认会选择与虚拟主机匹配的体系结构。
 - 在“安装工具”字段中，选择要用于安装 Guest 的自动安装工具。如果不使用自动安装，请将此字段留空。
3. 在“磁盘”部分，填写要用于客户端的虚拟磁盘的细节。在“URL”字段中，务必键入操作系统映像的路径。如果不这么做，创建的 Guest 的磁盘将会是空磁盘。
 4. 在“网络”部分，填写要用于客户端的虚拟网络接口的细节。将 MAC “”字段留空以生成 MAC 地址。
 5. 在“显卡”部分，填写要用于客户端的显卡驱动程序的细节。
 6. 安排创建 Guest 的时间，然后单击  以创建 Guest。
 7. 新虚拟 Guest 在成功创建后会立即启动。

也可以在 Uyuni Web UI 中的 Pacemaker 群集上添加虚拟 Guest。

Procedure: Creating a Cluster Managed Virtual Guest

1. 按照在群集某个节点上“” Guest 的过程操作，并遵循以下额外要求：
 - 确保“”字段处于选中状态。
 - 在“VM”“”字段中，键入由所有群集节点共享的文件夹的路径，Guest 配置将存储在该位置。
 - 确保每个磁盘都位于由所有群集节点共享的存储池上。

可实时迁移由群集管理的虚拟 Guest。

9.3. 使用 Xen 和 KVM 虚拟化

您可以直接在 Uyuni 中管理 Xen 和 KVM 虚拟化客户端。

To begin, you need to set up a virtual host on your Uyuni Server. You can then set up autoinstallation using AutoYaST or Kickstart for additional virtual hosts and for virtual guests.

This section also includes information about administering virtual guests after they have been installed.

9.3.1. 主机设置

The way that you set up Xen or KVM on a VM host depends on operating system you want to use on its associated guests:

- For SUSE operating systems, see the SLES Virtualization Guide available from <https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html>.
- 对于 Red Hat Enterprise Linux 操作系统，请参见适用于您所用版本的 Red Hat 文档。

借助“”公式，您可以初始化主机。有关详细信息，请参见 [client-configuration:virt-xenkvm.pdf](#)。

9.3.1.1. 背景信息

Uyuni uses libvirt to install and manage guests. You must have the libvirt-daemon package installed on your host. In most cases, the default settings are sufficient and you do not need to adjust them. However, if you want to access the VNC console on your guests as a non-root user, you need to perform some configuration changes. For more information about how to set up the VNC console, see the documentation for your operating system.

You need a bootstrap script on the Uyuni Server. The bootstrap script must include the activation key for your host. We also recommend that you include your GPG key for additional security. For more on creating a bootstrap script, see [Client-configuration > Registration-bootstrap](#).

When the bootstrap script is ready, use it to register the host with the Uyuni Server. For more information about client registration, see [Client-configuration > Registration-overview](#).

9.3.1.2. 初始化

使用公式初始化主机：

过程：初始化

1. 在 Uyuni Web UI 中，导航到主机的页面，然后单击选项卡。
2. 选择公式，然后单击[保存]。
3. 单击子选项卡。
4. 选中相应设置，然后单击[保存公式]。
5. 应用 Highstate，以使更改生效。
6. 重启动 salt-minion 服务以激活新配置：

```
systemctl restart salt-minion
```

9.3.2. 自动安装 VM Guest

您可以使用 AutoYaST 或 Kickstart 自动安装并注册 Xen 和 KVM Guest。

You need an activation key for the VM host you want to register the guests to, and for each guest. The activation key must have the provisioning and Virtualization Platform entitlements. For more information about creating activation keys, see [Client-configuration > Activation-keys](#).

If you want to automatically register the guests with Uyuni after installation, you need to create a bootstrap script. For more information about creating a bootstrap script, see [Client-configuration > Registration-bootstrap](#).

9.3.2.1. 创建可自动安装的发行套件

您需要在 VM 主机上创建可自动安装的发行套件，才能通过 Uyuni 自动安装客户端。可以在挂载的本地或远程

目录提供发行套件，也可以在以循环方式挂载的 ISO 映像中提供。

The configuration of the autoinstallable distribution differs depending on whether you are using a Red Hat Enterprise Linux or SUSE operating system on your guests. The packages for a Red Hat Enterprise Linux installation are fetched from the associated base channel. Packages for installing SUSE systems are fetched from the autoinstallable distribution. Therefore, for SUSE systems, the autoinstallable distribution must be a complete installation source.

表格 49. Paths for Autoinstallable Distributions

Operating System Type	Kernel Location	initrd Location
Red Hat Enterprise Linux	images/pxeboot/vmlinuz	images/pxeboot/initrd.img
SUSE	boot/<arch>/loader/initrd	boot/<arch>/loader/linux

在所有情况下，均需确保基础通道与可自动安装的发行套件匹配。

Before you begin, ensure you have a installation media available to your VM Host. It can be on a remote resource, a local directory, or a loop-mounted ISO image. Additionally, ensure that all files and directories are world-readable.

过程：创建可自动安装的发行套件

1. 在 Uyuni Web UI 中，导航到系统，自动安装，发行套件，然后单击 **[创建] [发行套件]**。
2. 在 **-----部分**，使用以下参数：
 - 在 **-----部分**，键入发行套件的唯一名称。请仅使用字母、数字、连字符 (-)、点 (.) 和下划线 (_)，并确保名称包含四个以上字符。
 - 在 **-----字段中**，键入安装源的绝对路径。
 - 在 **-----字段中**，选择与安装源匹配的通道。此通道用作非 SUSE 安装的软件包源。
 - 在 **-----字段中**，选择与安装源匹配的操作系统版本。
 - 在 **-----字段中**，键入在安装期间引导时要传递给内核的任何选项。The `install=` parameter and the `self_update=0` parameter are added by default.
 - 在 **-----部分**，键入在首次引导安装的系统时要传递给内核的任何选项。
3. 单击 **[创建] [可自动安装的发行套件]** 保存设置。

创建可自动安装的发行套件后，您可以导航到系统，自动安装，发行套件，然后选择要编辑的发行套件进行编辑。

9.3.2.2. 创建并上载自动安装配置文件

自动安装配置文件包含安装系统所需的所有安装和配置数据，还包含安装完成后需要执行的脚本。

在 Uyuni Web UI 中，导航到系统自动安装配置文件，单击 **[创建] [新 Kickstart] [配置文件]**，然后按照提示操作即可创建 Kickstart 配置文件。

您也可以手动创建 AutoYaST 或 Kickstart 自动安装配置文件。SUSE 提供了 AutoYaST 安装文件模板，您可以基于它们创建自己的自定义文件。您可以在 <https://github.com/SUSE/manager-build-profiles> 中找到这些模

板。

如果您要使用 AutoYaST 安装 SLES，则还需要包含以下代码段：

```
<products config:type="list">
<listentry>SLES</listentry>
</products>
```

- 有关 AutoYaST 的详细信息，请参见 [client-configuration:autoinst-profiles.pdf](#)。
- 有关 Kickstart 的详细信息，请参见 [client-configuration:autoinst-profiles.pdf](#) 或适用于您的安装的 Red Hat 文档。

过程：上载自动安装配置文件

- 在 Uyuni Web UI 中，导航到系统，自动安装，配置文件，然后单击 上 载 Kickstart/Autoyast [文件]。
- 在 部分，使用以下参数：
 - 在 字段中，为配置文件键入一个唯一的名称。请仅使用字母、数字、连字符 (-)、点 (.) 和下划线 (_)，并确保名称包含六个以上字符。
 - 在 字段中，选择您之前创建的可自动安装的发行套件。
 - 在 字段中，选择相关的 Guest 类型（例如 KVM Guest）。请勿在此处选择 Xen 。
 - 可选：如果您要手动创建自动安装配置文件，可以直接在 字段中键入相应内容。如果您已创建文件，请将 字段留空。
 - 在 字段中，单击 选择 ，然后使用系统对话框选择要上载的文件。如果文件成功上载， 字段中会显示相应文件名。
 - 字段中会显示上载的文件的内容。如果您需要编辑其内容，可以直接编辑。
- 单击 以保存更改并存储配置文件。

创建自动安装配置文件后，您可以导航到系统，自动安装，配置文件，然后选择要编辑的配置文件进行编辑。进行所需更改，然后单击 保存您的设置。



如果您更改了现有 Kickstart 配置文件的 ，则可能也会修改引导加载程序和分区选项，并可能重写任何自定义设置。请在更改前仔细查看 选项卡以校验这些设置。

9.3.2.3. 自动注册 Guest

自动安装 VM Guest 后，它们并不会注册到 Uyuni 中。如果您希望 Guest 在安装后立即自动注册，您可以在自动安装配置文件中添加一段用于调用引导脚本并注册 Guest 的内容。

此部分提供向现有 AutoYaST 配置文件添加引导脚本的指令。

有关创建引导脚本的详细信息，请参见 [Client-configuration > Registration-bootstrap](#)。有关如何针对

Kickstart 执行此操作的说明，请参见适用于您的安装的 Red Hat 文档。

过程：在 AutoYaST 配置文件中添加引导脚本

1. 确保引导脚本包含要注册的 VM Guest 的激活密钥，并且脚本位于主机上的 `/srv/www/htdocs/pub/bootstrap_vm_guests.sh` 中。
2. 在 Uyuni Web UI 中，导航到系统，自动安装，配置文件，然后选择要与此脚本关联的 AutoYaST 配置文件。
3. 在 `-----` 字段中，于文件末尾的 `</profile>` 结束标记前面添加以下代码段。务必在代码段中的示例 IP 地址 `192.168.1.1` 替换为 Uyuni 服务器的正确 IP 地址：

```
<scripts>
<init-scripts config:type="list">
<script>
<interpreter>shell</interpreter>
<location>
    http://192.168.1.1/pub/bootstrap/bootstrap_vm_guests.sh
</location>
</script>
</init-scripts>
</scripts>
```

4. 单击 **更新** 保存您的更改。



如果 AutoYaST 配置文件已包含 `<scripts>` 部分，请勿再添加，而是将引导代码段放在现有 `<scripts>` 部分内。

9.3.2.4. 自动安装 VM Guest

When you have everything set up, you can start to autoinstall your VM guests.



每个 VM 主机一次只能安装一个 Guest。如果您要安排多个自动安装，请务必安排合理的时间，确保下一个安装不会在现有安装完成前开始。如果某个 Guest 安装在另一个安装仍在进行时开始，则正在进行的安装可能会被取消。

1. 在 Uyuni Web UI 中，导航到系统，概览，然后选择要在其中安装 Guest 的 VM 主机。
2. Navigate to the Virtualization tab, and the Provisioning subtab.
3. 选择要使用的自动安装配置文件，并为 Guest 指定唯一的名称。
4. 选择代理（如果适用）并输入日程安排。
5. 要更改 Guest 的硬件配置文件和配置选项，请单击 **[高级选项]**。
6. 单击 **[安排自动安装并完成]** 以完成设置。

9.3.3. 管理 VM Guest

您可以使用 Uyuni Web UI 来管理 VM Guest，包括执行关机、重启动以及调整 CPU 和内存分配的操作。

To do this, you need your Xen or KVM VM host registered to the Uyuni Server, and have the `libvirtd` service running on the host.

在 Uyuni Web UI 中，导航到 **系统** > **系统列表**，然后单击要管理的 Guest 的 VM 主机。导航到 **VM Guest** 选项卡以查看所有注册到此主机中的 Guest，并访问管理功能。

For more information about managing VM guests using the Web UI, see [Reference > Systems](#).

Chapter 10. 虚拟主机管理器

虚拟主机管理器 (VHM) 用于收集各种客户端类型的信息。

VHM 可用于收集私有云或公有云实例，并将其分为不同的虚拟化组。以这种方式组织虚拟化客户端后，Taskomatic 便可收集客户端的相关数据以显示在 Uyuni Web UI 中。借助 VHM，您还可以在虚拟化客户端上使用订阅匹配。

您可以在 Uyuni 服务器上创建 VHM，并使用它来清点可用的公有云实例。您还可以使用 VHM 管理通过 Kubernetes 创建的群集。

- 有关将 VHM 与 Amazon Web Services 搭配使用的详细信息，请参见 [Client-configuration > Vhm-aws](#)。
- 有关将 VHM 与 Microsoft Azure 搭配使用的详细信息，请参见 [Client-configuration > Vhm-azure](#)。
- 有关将 VHM 与 Google Compute Engine 搭配使用的详细信息，请参见 [Client-configuration > Vhm-gce](#)。
- 有关将 VHM 与 Nutanix 搭配使用的详细信息，请参见 [Client-configuration > Vhm-nutanix](#)。
- 有关将 VHM 与 VMWare vSphere 搭配使用的详细信息，请参见 [Client-configuration > Vhm-vmware](#)。
- 有关将 VHM 与其他主机搭配使用的详细信息，请参见 [Client-configuration > Vhm-file](#)。

10.1. Virtual Host Manager and Amazon Web Services

您可以使用虚拟主机管理器 (VHM) 收集 Amazon Web Services (AWS) 中的实例。

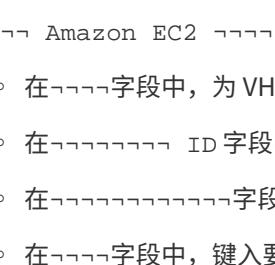
VHM 允许 Uyuni 获取并报告有关您的群集的信息。有关 VHM 的详细信息，请参见 [Client-configuration > Vhm](#)。

10.1.1. 创建 Amazon EC2 VHM

虚拟主机管理器 (VHM) 在 Uyuni 服务器上运行。

确保您已在 Uyuni 服务器上安装 virtual-host-gatherer-libcloud 软件包。

过程：创建 Amazon EC2 VHM

1. 在 Uyuni Web UI 中，导航到系统 > 虚拟主机管理器。
2. 单击  并从下拉菜单中选择 Amazon EC2。
3. 在  部分，使用以下参数：
 - 在 **名称** 字段中，为 VHM 键入自定义名称。
 - 在 **访问密钥 ID** 字段中，键入 Amazon 提供的访问密钥 ID。
 - 在 **机密访问密钥** 字段中，键入与 Amazon 实例关联的机密访问密钥。
 - 在 **地区** 字段中，键入要使用的地区。

- 在“区域”字段中，键入您的 VM 所在的区域。要使订阅匹配功能正常工作，就必须提供此信息。有关设置地区和区域的详细信息，请参见 [client-configuration:virtualization.pdf](#)。

4. 单击 保存更改并创建 VHM。
5. 在 页面中，选择新 VHM。
6. 在 页面中，单击 以清点新 VHM。

要查看已清点的对象和资源，请导航到 **系统 > 系统列表 > 虚拟系统**。

在 Amazon 公有云上运行的实例会向 Uyuni 服务器报告 UUID，其格式为一个 `i` 后跟 17 个十六进制数字：

```
I1234567890abcdef0
```

10.1.2. 虚拟主机管理器的 AWS 权限

出于安全原因，请始终为要执行的任务授予尽可能最小的权限。不建议对连接到 AWS 的用户使用具有过高权限的访问密钥。

为了让 SUSE Manager 从 AWS 收集所需的信息，VHM 需要相权限来说明 EC2 实例和地址。一种收集此信息的方法是专门为此任务创建一个新的 IAM 用户 (Identity and Access Management)，创建一个如下策略并关联到该用户：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

您可以通过限制对特定地区的访问来对权限施加更多限制。有关详细信息，请参见 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ExamplePolicies_EC2.html#iam-example-read-only。

10.2. Virtual Host Manager and Azure

您可以使用虚拟主机管理器 (VHM) 收集 Microsoft Azure 中的实例。

VHM 允许 Uyuni 获取并报告有关您的虚拟机的信息。有关 VHM 的详细信息，请参见 [Client-configuration > Vhm](#)。

10.2.1. 先决条件

要让您创建的 VHM 访问 Azure VM，需要为其指派正确的权限。

请以订阅管理员身份登录您的 Azure 帐户，并确保该 Azure 用户帐户和应用程序在正确的组中。应用程序所在的组决定了应用程序所拥有的角色，因而决定了其拥有的权限。

10.2.2. 创建 Azure VHM

虚拟主机管理器 (VHM) 在 Uyuni 服务器上运行。

确保您已在 Uyuni 服务器上安装 `virtual-host-gatherer-libcloud` 软件包。

过程：创建 Azure VHM

1. 在 Uyuni Web UI 中，导航到 **系统**，**虚拟主机管理器**。
2. 单击  并从下拉菜单中选择 Azure。
3. 在 **Azure** 部分，使用以下参数：
 - 在 **名称** 字段中，为 VHM 键入自定义名称。
 - 在 **订阅 ID** 字段中，键入在 Azure **设置** > **订阅** > **所有订阅** 页面中找到的订阅 ID。
 - 在 **租户 ID** 字段中，键入您在注册应用程序时获得的应用程序 ID。
 - 在 **租户 ID** 字段中，键入您在注册应用程序时获得的、由 Azure 提供的租户 ID。
 - 在 **机密密钥** 字段中，键入与 Azure 实例关联的机密密钥。
 - 在 **区域** 字段中，键入您的 VM 所在的区域。例如，如果位于西欧，则输入 `westeurope`。要使订阅匹配功能正常工作，就必须提供此信息。
4. 单击  保存更改并创建 VHM。
5. 在 **所有虚拟机** 页面中，选择新 VHM。
6. 在 **所有** 页面中，单击  以清点新 VHM。

要查看已清点的对象和资源，请导航到 **系统**，**系统列表**，**虚拟系统**。

10.2.3. 指派权限

如果未正确设置权限，您在运行 `virtual-host-gatherer` 时可能会收到如下所示的错误：

一般错误：[AuthorizationFailed] 对象 ID 为 'object_ID' 的客户端 'client_name' 无权在 '/subscriptions/not-very-secret-subscription-id' 范围执行操作 'Microsoft.Compute/virtualMachines/read'，或该范围无效。如果访问权限是最近授予的，请刷新您的身份凭证。

要确定正确的身份凭证，请在 Uyuni 服务器上的提示符处运行以下命令：

```
virtual-host-gatherer -i input_azure.json -o out_azure.json -vvv
```

input_azure.json 文件应包含以下信息：

```
[  
  {  
    "id": "azure_vhm",  
    "module": "Azure",  
    "subscription_id": "subscription-id",  
    "application_id": "application-id",  
    "tenant_id": "tenant-id",  
    "secret_key": "secret-key",  
    "zone": "zone"  
  }  
]
```

10.2.4. Azure UUID

在 Azure 公有云上运行的实例会向 Uyuni 服务器报告如下 UUID：

```
13f56399-bd52-4150-9748-7190aae1ff21
```

10.3. Virtual Host Manager and Google Compute Engine

您可以使用虚拟主机管理器 (VHM) 收集 Google Compute Engine (GCE) 中的实例。

VHM 允许 Uyuni 获取并报告有关您的虚拟机的信息。有关 VHM 的详细信息，请参见 [Client-configuration > Vhm](#)。

10.3.1. 先决条件

要让您创建的 VHM 可以访问 GCE VM，需要为其指派正确的权限。

以管理员身份登录您的 Google Cloud Platform 帐户，并使用 Cloud Identity and Access Management (IAM) 工具确保服务帐户拥有适当的角色。

10.3.2. 创建 GCE VHM

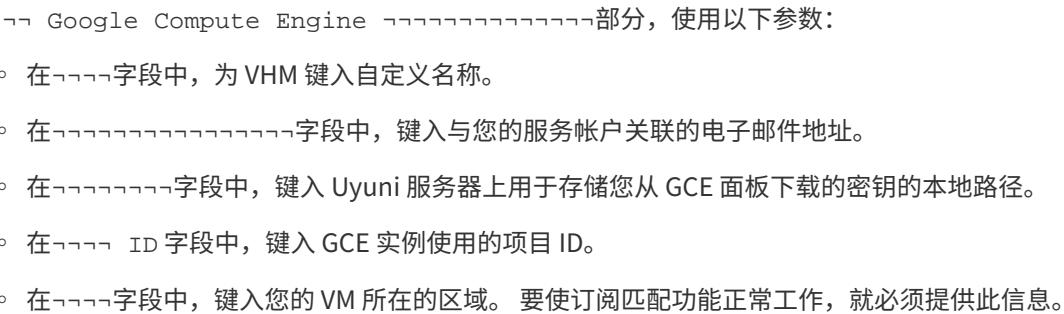
虚拟主机管理器 (VHM) 在 Uyuni 服务器上运行。

要运行 VHM，需要打开端口 443 以使您的 Uyuni 服务器可访问客户端。

确保您已在 Uyuni 服务器上安装 `virtual-host-gatherer-libcloud` 软件包。

开始前，请登录 GCE 面板并下载证书文件。将此文件存储在 Uyuni 服务器本地，并记下路径。

过程：创建 GCE VHM

1. 在 Uyuni Web UI 中，导航到系统，虚拟主机管理器。
2. 单击  并从下拉菜单中选择 Google Compute Engine。
3. 在  部分，使用以下参数：
 - 在  字段中，为 VHM 键入自定义名称。
 - 在  字段中，键入与您的服务帐户关联的电子邮件地址。
 - 在  字段中，键入 Uyuni 服务器上用于存储您从 GCE 面板下载的密钥的本地路径。
 - 在  字段中，键入 GCE 实例使用的项目 ID。
 - 在  字段中，键入您的 VM 所在的区域。要使订阅匹配功能正常工作，就必须提供此信息。
4. 单击  保存更改并创建 VHM。
5. 在  页面中，选择新 VHM。
6. 在  页面中，单击  以清点新 VHM。

要查看已清点的对象和资源，请导航到系统，系统列表，虚拟系统。

10.3.3. 指派权限

如果未正确设置权限，您在运行 `virtual-host-gatherer` 时可能会收到如下所示的错误：

```
错误: {'domain': 'global', 'reason': 'forbidden', 'message': "需要
'compute.zones.list' 权限, 'projects/project-id'"}
错误: 无法使用指定的身份凭证连接 Google Compute Engine 公有云。
```

要确定正确的身份凭证，请在 Uyuni 服务器上的提示符处运行以下命令：

```
virtual-host-gatherer -i input_google.json -o out_google.json -vvv
```

`input_google.json` 文件应包含以下信息：

```
[  
  {  
    "id": "google_vhm",  
    "module": "GoogleCE",  
    "service_account_email": "mail@example.com",  
    "cert_path": "secret-key",  
    "project_id": "project-id",  
    "zone": "zone"  
  }  
]
```

10.3.4. GCE UUID

在 Google 公有云上运行的实例会向 Uyuni 服务器报告如下 UUID：

152986662232938449

10.4. 使用 Nutanix 虚拟化

您可以通过在 Uyuni 中设置虚拟主机管理器 (VHM) 来使用 Nutanix AHV 虚拟机。开始前，您需要在 Uyuni 服务器上设置 VHM，然后清点可用的 VM 主机。

10.4.1. VHM 设置

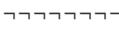
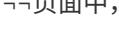
虚拟主机管理器 (VHM) 在 Uyuni 服务器上运行。

确保您已在 Uyuni 服务器上安装 `virtual-host-gatherer-Nutanix` 软件包。

要运行 VHM，必须打开端口 9440 以使您的 Uyuni 服务器可访问 Nutanix Prism Element API。

过程：创建 Nutanix VHM

1. 在 Uyuni Web UI 中，导航到系统 > 虚拟主机管理器。
2. 单击 **[创建]**，然后选择 Nutanix AHV。
3. 在 **Nutanix AHV** 部分，使用以下参数：
 - 在 **名称** 字段中，为 VHM 键入自定义名称。
 - 在 **完全限定域名** 字段中，键入完全限定的域名 (FQDN) 或主机的 IP 地址。
 - 在 **端口** 字段中，键入要使用的 Prism Element API 端口（例如，9440）。
 - 在 **用户名** 字段中，键入与 VM 主机关联的用户名。
 - 在 **口令** 字段中，键入与 VM 主机用户关联的口令。

4. 单击  保存更改并创建 VHM。
5. 在  页面中选择新 VHM。
6. 在  页面中，单击  以清点新 VHM。

要查看已清点的对象和资源，请导航到 **系统 > 系统列表 > 虚拟系统**。



Connecting to the Nutanix Prism API server from a browser using HTTPS can sometimes log an invalid certificate error. If this occurs, refreshing the data from the virtual host manager fails. A valid SSL certificate (not self-signed) is required on your Nutanix API server. If you are using a custom CA authority for your Nutanix SSL certificate, copy the custom CA certificate to `/etc/pki/trust/anchors` on the Uyuni Server.

Re-trust the certificate by running the `update-ca-certificates` command on the command line, and restart the spacewalk services.

创建并配置好 VHM 后，Taskomatic 即会自动运行数据收集过程。如果您要手动进行数据收集，请导航到 **系统 > 虚拟主机管理器**，选择适当的 VHM，然后单击 。

Uyuni 随附了一个名为 `virtual-host-gatherer` 的工具，可以使用相应 API 连接到 VHM 并请求虚拟主机的相关信息。`virtual-host-gatherer` 计算机会维护可选模块的概念，每个模块可启用一个特定的 VHM。Taskomatic 会在夜间自动调用此工具。`virtual-host-gatherer` 工具的日志文件位于 `/var/log/rhn/gatherer.log`。

10.5. 使用 VMWare 虚拟化

您可以在 Uyuni 中设置虚拟主机管理器 (VHM) 来使用 VMWare vSphere 虚拟机，包括 ESXi 和 vCenter。

开始前，您需要在 Uyuni 服务器上设置 VHM，然后清点可用的 VM 主机。之后，Taskomatic 便可以开始使用 VM API 收集数据。

10.5.1. VHM 设置

虚拟主机管理器 (VHM) 在 Uyuni 服务器上运行。

要运行 VHM，需要打开端口 443 以便您的 Uyuni 服务器可访问 VMWare API。

VMWare 主机使用访问权限角色和权限来控制对主机和 Guest 的访问。请确保您要让 VHM 清点的任何 VMWare 对象或资源均至少具有  权限。如果您要排除任何对象或资源，请将它们标记为 。

当您向 Uyuni 添加新主机时，需考虑是否需要让 Uyuni 清点已指派给用户和对象的角色和权限。

有关用户、角色和权限的详细信息，请参见 VMWare vSphere 文档，网址为：<https://docs.vmware.com/en/VMware-vSphere/index.html>

过程：创建 VMWare VHM

1. 在 Uyuni Web UI 中，导航到系统 > 虚拟主机管理器。
2. 单击  [创建]，然后选择 VMWare。
3. 在 VMWare 配置部分，使用以下参数：
 - 在 VHM 字段中，为 VHM 键入自定义名称。
 - 在 FQDN 字段中，键入完全限定的域名 (FQDN) 或主机的 IP 地址。
 - 在 API 端口字段中，键入要使用的 ESXi API 端口（例如，443）。
 - 在 用户名 字段中，键入与 VM 主机关联的用户名。
 - 在 口令 字段中，键入与 VM 主机用户关联的口令。
4. 单击  [保存] 保存更改并创建 VHM。
5. 在 页面中选择新 VHM。
6. 在 页面中，单击  [刷新] [新数据] 以清点新 VHM。

要查看已清点的对象和资源，请导航到系统 > 系统列表 > 虚拟系统。



有时，在浏览器中使用 HTTPS 连接 ESXi 服务器可能会发生 SSL 错误。如果发生此情况，刷新来自虚拟主机服务器的数据将会失败。要纠正该问题，请解压缩来自 ESXi 服务器的证书，然后将其复制到 /etc/pki/trust/anchors。在命令行上运行 update-ca-certificates 命令以重新信任证书，然后重启 spacewalk 服务。

创建并配置好 VHM 后，Taskomatic 即会自动运行数据收集过程。如果您要手动进行数据收集，请导航到系统 > 虚拟主机管理器，选择适当的 VHM，然后单击  [刷新] [新数据]。

Uyuni 随附了一个名为 virtual-host-gatherer 的工具，可以使用相应 API 连接到 VHM 并请求虚拟主机的相关信息。virtual-host-gatherer 计算机会维护可选模块的概念，每个模块可启用一个特定的 VHM。Taskomatic 会在夜间自动调用此工具。virtual-host-gatherer 工具的日志文件位于 /var/log/rhn/gatherer.log。

10.5.2. 在 VMWare 上对 SSL 错误进行查错

如果您在配置安装的 VMWare 时遇到 SSL 错误，需要下载 VMWare 提供的 CA 证书文件，并在 Uyuni 上信任该证书。

过程：信任 VMWare CA 证书

1. 从您安装的 VMWare 中下载 CA 证书。您可以通过登录 Uyuni Web UI 并单击  [下载] [可信 CA] [证书] 来实现此目的。
2. 如果下载的 CA 证书文件为 .zip 格式，请解压缩该存档文件。证书文件的扩展名有多种。例如，certificate.0。
3. 将证书文件复制到 Uyuni 服务器上并保存到 /etc/pki/trust/anchors/ 目录中。
4. 将复制的证书的文件名后缀改为 .crt 或 .pem。
5. 在 Uyuni 服务器上的命令提示符处更新 CA 证书记录：

```
update-ca-certificates
```

10.6. 使用其他第三方提供者虚拟化

如果您要使用 Xen、KVM 或 VMware 以外的第三方虚拟化提供者，可以将 JSON 配置文件导入到 Uyuni 中。

同样，如果您安装的 VMWare 不提供直接访问 API 的功能，基于文件的 VHM 可以为您提供基本的管理功能。



此选项用于导入使用 `virtual-host-gatherer` 工具创建的文件，不可用于导入手动创建的文件。

过程：导出和导入 JSON 文件

1. 在 VM 网络上运行 `virtual-host-gatherer` 以导出 JSON 配置文件。
2. 将产生的文件保存到 Uyuni 服务器可访问的位置。
3. 在 Uyuni Web UI 中，导航到 **系统 > 虚拟主机管理器**。
4. 单击 **[新建]**，然后选择 **-----**。
5. 在 **-----** 部分，使用以下参数：
 - 在 **-----** 字段中，为 VHM 键入自定义名称。
 - 在 **URL** 字段中，键入导出的 JSON 配置文件的路径。
6. 单击 **[新建]** 保存更改并创建 VHM。
7. 在 **-----** 页面中，选择新 VHM。
8. 在 **-----** 页面中，单击 **[刷新数据]** 以清点新 VHM。

列表 3. 例如：导出的 JSON 配置文件：

```
{
  "examplevhost": {
    "10.11.12.13": {
      "cpuArch": "x86_64",
      "cpuDescription": "AMD Opteron(tm) 处理器 4386",
      "cpuMhz": 3092.212727,
      "cpuVendor": "amd",
      "hostIdentifier": "'vim.HostSystem:host-182'",
      "name": "11.11.12.13",
      "os": "VMware ESXi",
      "osVersion": "5.5.0",
      "ramMb": 65512,
      "totalCpuCores": 16,
      "totalCpuSockets": 2,
      "totalCpuThreads": 16,
    }
  }
}
```

```
        "type": "vmware",
        "vms": {
            "vCenter": "564d6d90-459c-2256-8f39-3cb2bd24b7b0"
        }
    },
    "10.11.12.14": {
        "cpuArch": "x86_64",
        "cpuDescription": "AMD Opteron(tm) 处理器 4386",
        "cpuMhz": 3092.212639,
        "cpuVendor": "amd",
        "hostIdentifier": "'vim.HostSystem:host-183'",
        "name": "10.11.12.14",
        "os": "VMware ESXi",
        "osVersion": "5.5.0",
        "ramMb": 65512,
        "totalCpuCores": 16,
        "totalCpuSockets": 2,
        "totalCpuThreads": 16,
        "type": "vmware",
        "vms": {
            "49737e0a-c9e6-4ceb-aef8-6a9452f67cb5": "4230c60f-3f98-2a65-f7c3-600b26b79c22",
            "5a2e4e63-a957-426b-bfa8-4169302e4fdb": "42307b15-1618-0595-01f2-427ffcd88e",
            "NSX-gateway": "4230d43e-aafe-38ba-5a9e-3cb67c03a16a",
            "NSX-l3gateway": "4230b00f-0b21-0e9d-dfde-6c7b06909d5f",
            "NSX-service": "4230e924-b714-198b-348b-25de01482fd9"
        }
    }
}
```

有关详细信息，请参见 Uyuni 服务器上 `virtual-host-gatherer` 的手册页：

man virtual-host-gatherer

该软件包的 README 文件提供有关超级管理程序----的背景信息及其他信息：

/usr/share/doc/packages/virtual-host-gatherer/README.md

手册页和 README 文件还包含示例配置文件。

Chapter 11. 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".